Security Applications for Converging Technologies - Impact on the Constitutional State and the Legal order

Teeuw, W.; Vedder, A.H.; Custers, B.H.M.; Dorbeck-Jung, B.R.; Faber, E.; Iacob, S.; Koops, E.J.; Leenes, R.E.; de Poot, H.; Rip, A.; Vudisa, J.N.

Publication date:
2008

Document Version
Publisher's PDF, also known as Version of record

Telematica
Instituut

Security Applications for Converging Technologies

Impact on the constitutional state and the legal order

Wouter B. Teeuw (Ed.)
Anton Vedder (Ed.)

With contributions from:
Bart Custers
Bärbel Dorbeck-Jung
Edward Faber
Sorin Iacob
Bert-Jaap Koops
Ronald Leenes
Henk de Poot
Arie Rip
Jacques Vudisa

Telematica
Instituut

TELEMATICA INSTITUUT, ENSCHEDE, REPORT TI/RS/2007/039

Synopsis:

In this study we investigate the impact of converging technologies on legal practice and criminology in a forward looking study intended for practitioners and policy makers in the field of legislation, crime prevention, and law enforcement. We look at a 15 years timeframe and discuss the scientific and technical progress in various domains as well as the ethical, legal, and policy dilemmas involved.

Table of Contents

Abbreviations used

CT	Converging Technologies
DBS	Deep Brain Stimulation
DC	Dutch Constitution (Grondwet)
DCC	Dutch Criminal Code (Wetboek van Strafrecht)
DCCP	Dutch Code of Criminal Procedure (Wetboek van Strafvordering)
DNA	Desoxyribo Nucleic Acid
ECHR	European Convention of Human Rights and Fundamental Freedoms
ECtHR	European Court of Human Rights
EEG	Electroencephalogram
fMRI	functional Magnetic Resonance Imaging
GPS	Global Positioning System
ICT	Information and Communication Technology
NBIC	Nano-, Bio-, Information and Cognitive science and technology
NFB	Neurofeedback
RFID	Radio Frequency Identification
STM	Scanning Tunnelling Microscope
TMS	Transcranial Magnetic Stimulation

Summary

This study on *converging technologies* is a forward looking study intended for practitioners and policy makers in the field of security, legislation, crime prevention, and law enforcement. We use three selected cases where converging technologies may fit in: monitoring and immediate action, forensic research and profiling and identification. This study takes the technological developments as its starting point. Four converging technologies are distinguished: nanotechnology, biotechnology, information technology and cognitive technologies. We estimated what the developments in the field of converging technologies would be, translated them to the application domain mentioned and then set out to assess the trends in the social and normative impact of those developments.

In our approach, we started with the technology developments (independent of applications), wrote scenarios based on these developments (independent of an impact analysis), and then analysed the normative and social impacts of these scenarios in the form of eight trends that we consider important. These results may be used to start debates, either internally (the role of relevant Ministries, the impact of their policy on scenarios) or externally (social debate). In this way the technology forecasts, scenarios and impact analysis may be used to shape new policies, which in turn will possibly influence the technology developments.

Consequently, this report consists of three parts. The first part describes the state of the art and future expectations on nano-, bio-, ICT and cognitive science and technology, as well as their convergence. The second part describes the (future) applicability of converging technologies to our application domain, in particular the three cases. This part ends with scenarios that are used as a means to 'visualize' the developments and an input for the impact analysis. In the third part the scenarios are analysed on their ethical, legal and social implications. This part describes the major social and normative trends we observe.

Nanotechnology

Nanotechnology is a generic term that encompasses technologies that operate with entities, materials and systems of which at least one characteristic size dimension is between 1 and 100 nm. A key aspect is the occurrence of specific properties because of the nanoscale (e.g. large surface areas, quantum effects). Commonly, three main areas are distinguished:

- Nano-enabled materials and nano-structured surfaces. Nano materials technology is currently the most mature of the nano-technologies and with the highest penetration in commercial products such as cosmetics, coatings, textiles, adhesives, catalysts, and reinforced materials.
- Micro/nano-electronics. Nano-electronics shows a mixture of ongoing improvements of established performance (as with hard disks and MRAM memories), nano-enabled developments (as in large-area electronics) which are ready for use but do not always have the right performance yet, and speculations based on new discoveries and proof-of-principle only.

– Bionanotechnology and nanomedicine. DNA micro arrays are available for fast throughput analysis, and lab-on-a-chip technology is in place, even if not taken up widely. Sensors and actuators (MEMS/NEMS) are an important growth area, in particular biosensors 'on the spot' which will replace taking of samples for measurement in laboratories (so-called 'point of care' analysis). Targeted drug delivery is an important promise.

An interesting attempt at an overall view for future developments is the four-generation scheme of Mihail Roco, senior adviser to the US National Nanotechnology Initiative. The first generation has been the passive nanostructures. The second generation, reactive ('smart') materials and structures, are capable of changing their properties in response to different external changes (like temperature, electro-magnetic fields, humidity, etc.), and combine sensing and acting. The next step is to integrate some computing, so that choices can be made and acted upon. Nanotechnology will enable further functions and performances. The fourth generation will be molecular nanosystems, e.g., molecular devices 'by design'.

Biotechnology

Biological technology is technology based on biology, the study of life. Before the 1970s, the term biotechnology has mainly been used in the food processing and agriculture industries. Since then, the term biotechnology is also used for engineering techniques related to the medicine field, like the engineering of recombinant DNA or tissue culture.

Nowadays, the term biotechnology is used in a much broader sense to describe the whole range of methods to manipulate organic matter to meet human needs. Biotechnology has developed far beyond seed improvement and genetically modified oats, rice, etc. Many of today's biotechnology applications have a medical or therapeutic focus. This has also drawn the interest of criminologists to look for medication and therapies from a systems biological, biochemical, neurobiological, or biopsychiatrical perspective.

In the coming years, genetic analysis is likely to improve both with regard to accuracy, speed, and ease of operation. An example could be the implementation of gene passports. Also, synthetic biology and synthetic medicine may lead to developing agents with various functional abilities, such as preventing pathogens from entering the body, exploit pathogens' vulnerabilities, or enhance the immune response to new pathogens. Biomedical engineering will continue to advance in the direction of producing more complex artificially grown tissues, such as cartilage. Gene therapy, and generally the modification of human genes will continue to be a major research area. However, the extraction of personal characteristics from genetic material for identifying or other purposes is far away because DNA is a complex matter. It raises the question whether simpler biological clues to understand behaviour, health or body functioning are available.

Information technology

Information technology encompasses all the technologies related to the logical and physical definition, design and implementation of systems and applications for data acquisition, storage, processing, transmission, and management. Since almost all aspects of the current human activities heavily rely on ICT solutions, it is impossible to give a

comprehensive view of all state-of-the-art applications. We considered the most relevant for the current study.

On the application layer, there is a current trend to create ambient intelligence through smart, context-aware surroundings, smart devices (e.g. automatic selection of washing programs based on the type and quantity of laundry or the pre-tension of seat belts when an impact seems imminent). In camera surveillance systems there is a data explosion of an ever increasing sensor network calls for automatic recognition (identification or verification) of persons based on biometric features, and event detection as a form of pre-selection for human supervisors. Autonomy is key in future applications. A wide adoption of household robotics is expected. Applications are expected that allow observers of large datasets some visualisation. The sensor networks will be spread around in the living body, in vitro in living cells, in the air to probe the atmosphere, or on earth to sniff, listen, film, etc. And the quality of the data collected, will allow better understanding of many complex systems. For these systems to be really understood, these experience interfaces need to be available.

One of the bottlenecks in ICT may become the complexity of handling large volumes of data. That is, the data volumes may grow faster than the process capacity. For example, a single human genome is already 6 Gigabit of data. This volume of data is still small compared with the possibilities of millions of RFID tags being scanned in logistic streams, the number of sensors growing enormously, and persons being continuously on-line with human-computer interfaces becoming more friendly due to sensors, speech technology, etc. Quantum computing may be a solution for this problem, because quantum computing power is supposed to scale in an exponential way with the number of processors (whereas current computers scale in a linear way). However, quantum computers are judged as a long term and uncertain development.

Cognitive technology

For the purposes of this document the most relevant aspects of cognitive sciences are the study of structures, functions, and processes that define, implement, or describe the perception and interpretation of stimuli, decision making, and experiencing of mental states.

Computational theories of cognition propose mathematical or algorithmic description of neural processes. These theories are developed based on observed in vivo analysis of reactions to stimuli and ex vivo analysis of neural structures. Brains however are complex to model. Empirical theories of cognition start from observed behaviours (or subjects' self-reports), and psychological assessments and propose models that logically explain the observed behaviours and psychological properties. The theories concerning higher-level cognitive processes, such as mind states, experience, and consciousness are mostly empirical, and some quite speculative. Within the artificial intelligence (AI) field many analytic, logic, statistic, and algorithmic models have been proposed for learning, reasoning, categorization and clustering, pattern discovery and recognition, data correlation, etc. But there are few agreements as to how they are sound models for biological intelligence.

Futurists believe in unravelling the secrets of human cognition and consciousness before 2020, but cognitive scientists are more sceptical. It is unlikely that the high-level cognitive functions (such as intentions formation, creative problem solving, and consciousness) will be fully explained. The general opinion is that 'brain reading' is over

exaggerated. Techniques like fMRI and EEG are very valuable for pathological purposes, and brain stimulation is used for medical purposes as well, but there is too much noise in brain signals to allow the interpretation of, e.g., thoughts. Nonetheless, in the cognitive area there seems to be a lot of 'low-hanging fruit' to be applied for security purposes. Probably much more can be done with facial expressions. We know a great deal about emotions. Inferring emotions from facial expressions is likely to become accurate enough for using in a wide range of applications.

NBIC Convergence

All four NBIC fields are multidisciplinary in their own. Convergence is therefore a process, and not a property of this collection of technologies. The process leads to new paradigms in application areas. These shifts can not be forecasted, but we argue that convergence occurs naturally along two dimensions: structures, and functionalities, as follows (see Figure 1):

1 Nanotechnology and biotechnology deal with *structures* that have different underlying nature, but evolve toward comparable architectural complexity.

2 Cognitive sciences and ICT deal with *functionalities* implemented on structures of a different nature, but evolve toward comparable algorithmic complexity.

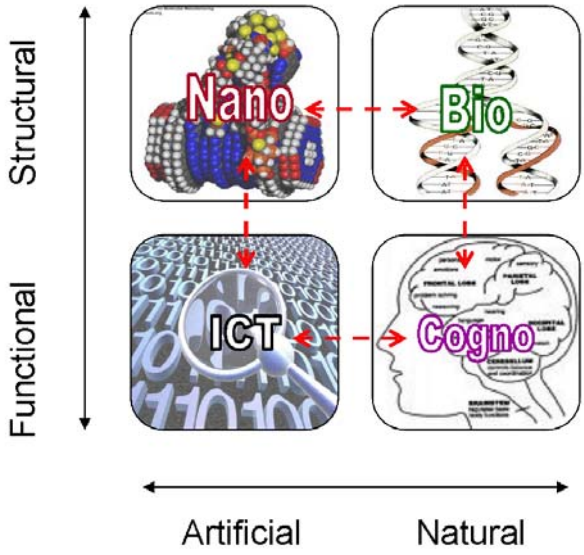


Figure 1: A model for natural convergence along two dimensions.

The main effect of these convergence processes is the achievement of reciprocal compatibility between the converging technologies.

Application of convergent technologies

Since convergence is a process, it becomes visible through applications. To focus the discussion on the meaning of convergent technologies for our application domain (i.e., the area of security and crime control), we restrict ourselves to three cases:

– Case 1: Monitoring and following objects or persons and remote intervention in case of undesired movements and relocations (in short: *Monitoring and immediate action*);
– Case 2: Improving and developing forensic trace analysis (in short: *Forensic research*);
– Case 3: Profiling, identifying and observing persons with an assumed security risk (in short: *Profiling and identification*).

For each case, we look into the expectations for the short (5 year), mid (10 year) and long term (15 year).

Monitoring and immediate action deals with e.g. positioning and/or communication technologies like GPS or RFID tags can be used to track and trace objects or persons. A special case is the tagging of persons as currently happens in experiments with prisoners. Besides monitoring people to prevent them from doing wrong, one may also monitor persons to protect them. The general belief is that people are willing to give up privacy in favour of individual or collective security. However, that does not necessarily mean that privacy becomes less important. Currently, mainly ICT technology seems to be used for monitoring and (remote) immediate action. Convergent technologies will allow the on-line registration of many variables (e.g. body sensors), advanced risk assessment by the combination of bio-, cognitive- and ICT indicators, and restraining persons in well-defined cases. Besides, we have to deal with the issue of tampering. In our forecast, we suggest that the following applications in monitoring and immediate action will be technically feasible by 2022:

– Individually worn sensors, in particular tagging prisoners or persons being detained during her majesty's pleasure (the Dutch 'TBS') with an implanted RFID chip (short term).
– Wearable personal monitoring devices with data recording and on-line communications capability (short term).
– Tracking and tracing individuals in public civic areas.
– Implants (or prostheses) that mimic or even augment human biological functions, but no selective memory erasure and no behaviour manipulation by brain implants.
– Blocking cars automatically based on sensor information (short term).
– Objects (e.g. clothes) that respond to external stimuli (like location, heart beat).
– Wireless Internet available worldwide (short term).

In forensic research, new technologies make it possible to establish new or radically enhanced ways of producing evidence. An example is using DNA material for identification. New technologies may even be required because of the necessity to analyze minute traces (level of molecules). NBIC technology may completely change the way of working. For example, due to lab-on-a-chip technology the analysis results may steer the search for traces. The miniaturising and commodification also means that techniques that used to be available to large institutions only, become available to individuals, who can do the same analyses. 'Social software' may be used to involve larger communities for collecting information. Relevant technologies for the coming years include portable analysis instruments, large-scale databases, single molecule detection, biomarkers, DNA profiling and 3D imaging of crime scenes. In our forecast, we suggest the following applications in forensic research will be technically feasible by 2022:

– Rapid forensic evaluations from very small amounts of materials (short term).
– The use of new families of (miniaturized) highly selective, accurate and sensitive biological sensors.
– Computational devices –like 'lab-on-a-chip'– becoming commercially available.

– Objects (e.g. clothes) that respond to external stimuli like the availability of specific (biological) substances.
– Powerful wearable computers / laboratories (short term).
– 3D visualisation of crime scenes.
– Resistant textiles, showing hardly any traces (long term).

To search for persons with an assumed risk for society, profiling can be used. A risk analysis may be based on available information from any 'intelligence' applications. Then, profiling also becomes the prediction of (or anticipation on) expected behaviour based on all available information. Identification also deals with looking for a specific person –whose identity is known– in the crowd. In general, people leave more and more traces in the virtual world by browsing on Internet, using their mobile phone, carrying RFID tags, or being observed by cameras. The amount of data registered about persons and objects is growing enormously. For this case, information processing applications are expected and face recognition is important. 'Brain reading' applications are far away, and it is not expected for the coming 15 years to derive behaviour from a gene structure. Nonetheless, combining information from all kinds of bodysensors and cognitive analyses may make it possible to predict risk factors. In our forecast, we suggest the following applications in profiling and identification will be technically feasible by 2022:
– Widespread use of (real-time) surveillance and monitoring of humans and environments / presence of sensors in public areas.
– Unobtrusive camera surveillance and sensor networks with increasingly small sizes (short to middle term).
– Widespread use of RFID tags (e.g. in the retail sector) that can be used to track persons (short term).
– Massive databases, e.g. holding genomic information (short term).
– Coupling of databases/sensor information, improved search capabilities and artificial intelligence to logically process collected information.
– Biometrics –probably combined with other available (context) information– widely applied for security functions (but no brain reading).
– Hands-free human-computer interaction enabling input devices with fast and unobtrusive data capturing.
– Genetic screening for e.g. clinical pictures, but not for predicting behaviour.
– Secure personal data transfer, like anonymous transactions or identifier removal.

Scenarios

We have sketched four scenarios to visualise the future application of converging technologies within our application domain. The scenarios have been based on the expected (realistic) technology developments for the coming 15 years. The scenarios have been written from a technology point of view and are a means to allow an impact analysis of converging technologies. We used two uncertainties to sketch four typical and related scenarios:
1 The degree of information sharing that can be realized between stakeholders involved in security enforcement chain.
2 The degree of information processing: the capacity to store and analyse the growing amount of collected data.

In all scenarios the technology becomes 'invisible', which results in a move towards what we have labelled 'ambient intelligent public security enforcement'. Depending on how the two uncertainties develop in the future (for the scenarios we choose the extremes limited versus extensive), four different scenarios are possible (see Figure 2). We have

characterised these scenarios with the terms ‘Pre-crime’, ‘Social crime control’, ‘Lab in your pocket’ and ‘Collectors mania’. In ‘Collectors mania’ we observe reactive authorities, collecting information and evidence to be used on purpose. In ‘Pre-crime’ we observe a shift from a reactive towards a proactive government, using technology to anticipate on and prevent crime. The technology is enabling in the sense of supporting the developments in society towards prevention. The two other scenarios focus on specific applications and show how converging technologies may be a driver for new ‘paradigms’ in the security application field. They sketch a more participatory role of citizens in forensic research (‘Lab in your pocket’) or surveillance and law enforcement (‘Social crime control).

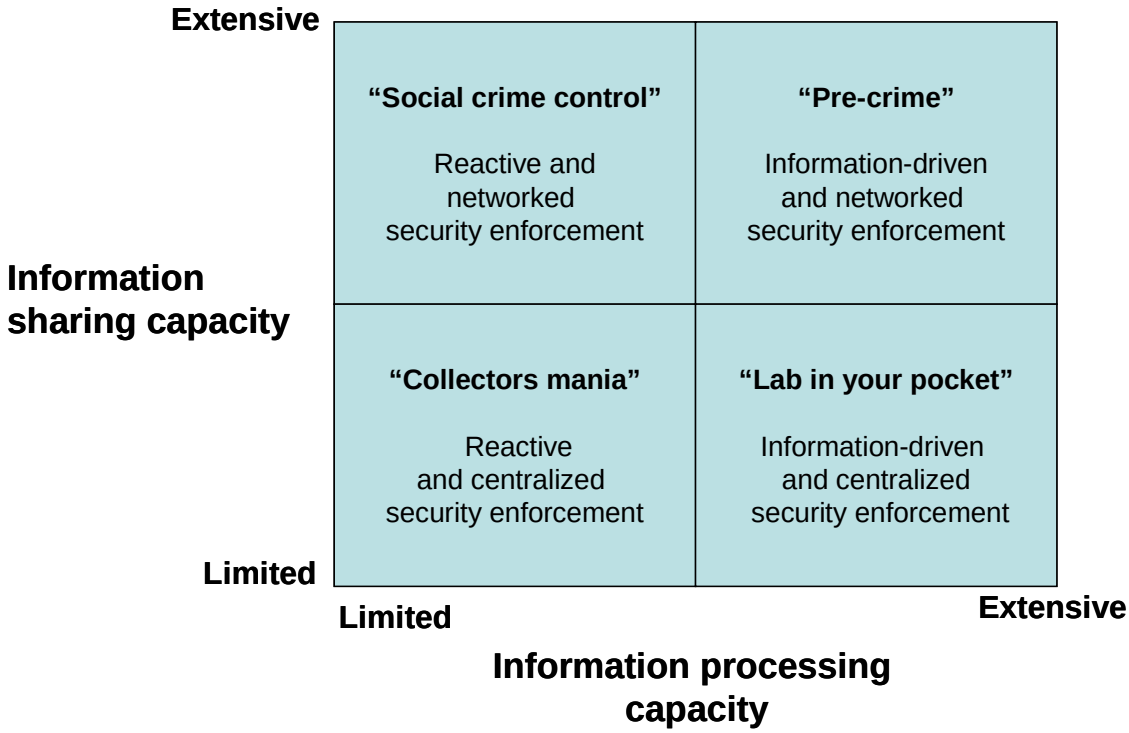


Figure 2: Using two key uncertainties to build four ‘related’ scenarios.

The ‘pre-crime’ scenario is closely related to the profiling and identification case. It shows a shift towards prevention, from a reactive towards an information-driven proactive environment. Sensors are available everywhere and the information can be processed to take the right decisions. The government policy is anticipation on and prevention of criminality. Characteristics of the future situation are:

- Persons with an assumed security risk are monitored;
- The widespread use of RFID tags in or on de body for monitoring and identification purposes;
- The use of sensors (video surveillance, body sensors, brain scans, etc.) for e.g. aggression detection;
- The coupling of public and private information sources for an all-embracing analysis of a person’s behaviour and relationships;
- Actuators that restrict persons in their movements.

The ‘social crime control’ scenario is closely related to the monitoring and immediate action case. The scenario shows a paradigm shift with respect to (public-private) collaboration. Due to collaboration with private partners or citizens, small-scale,

individual monitoring is possible in this scenario. It enables therapy close to someone's home environment ('prison without walls'). Characteristics of the future situation are:
- Individual tracking and tracing of persons with a seamless handover from outdoor (GPS) to indoor (camera surveillance) or public to private systems;
- Entire population is assessed for tendencies to criminal behaviour;
- Blurring borders between virtual and physical behaviour;
- Citizens participate in tracing criminals and law enforcement; mutual observation and social control of citizens.

The 'lab in your pocket' scenario is closely related to the forensic research case. The scenario shows a paradigm shift with respect to the availability of specialised equipment for the ordinary man. The scenario has been based on (trace) analysis tools becoming small, quick, accurate, low-priced and handy. Herewith their results steer and change the (forensic) research process. Also, these tools become a commodity and therefore are used by private researchers (or criminals) as well. Characteristics of the future situation are:
- Nano sprayers to detect the smallest traces;
- 3D reconstruction of crime scene;
- Lab-on-a-chip technology available to everyone;
- Global sensor information becomes available as a service to citizens (tracking locations, camera data, etc.);
- Real-time analysis of data, e.g., for database matches (DNA, face recognition), trace analysis, etc.

In the 'collector's mania' scenario, none of the three application cases has a position of favour. The scenario extrapolates the current, somewhat reactive (rather than anticipatory) processes towards the future. This does not mean, however, that the scenario is less advanced because the NBIC technologies still advance. Characteristics of the future situation are:
- Much information is collected, arranged, presented etc. In particular, the data is used for searching afterwards;
- Tasks shift from public partners to private partners (services) and eventually to citizens, but more on a service rather than collaboration base;
- Enhanced camera surveillance, e.g., it is possible to distinguish voluntary or forced behaviour.

Impact analysis

Obviously, the technological developments, applications, and scenarios are closely related to social and normative issues. Eight possible social and normative, i.e., moral and legal, trends may condition the impact of the use of converging technologies for security tasks and law enforcement. The social trends are concerned with implications of increasing polycentric and multi-actor crime surveillance and challenges to governability. The normative ones focus on new privacy concerns, issues of self-control versus control by others, the moral foundations of the law and the legitimacy of new forms of regulation. It should be noted that these trends will often overlap and intertwine in real practice. In order to highlight possible salient developments, it is, however, useful to distinguish them *in abstracto*.

The approach with regard to the impact analysis and assessment in this report is one of several possible alternatives. We have projected a certain future technological performance, in order to consider possible impacts. In discussing such impacts and assessing them, we had to *quasi* reify that technological future; assume that it would be

there, somehow, without further discussion. The implication is that a discussion of social, moral and legal impacts, here of converging technologies, will have an exemplary character rather than offering a picture of the future world. Still, this can draw attention to issues and challenges that deserve to be paid attention to in the here and now.

Eight trends have been distinguished:

1 Shifts in data collection and data processing: More and more data are being created; they are disseminated more widely, to a larger number of parties; access to data is made easier for the government, and control over these data is becoming increasingly difficult for data subjects. The consequence of this trend is that, even with the same investigative powers, governmental authorities are in a position to collect and use significantly more data about citizens than before, and this increase is not only quantitative but also qualitative. This in turn enables the government, in principle, to know better than ever before what citizens, including criminals and terrorists but also 'the man in the street', are doing.

2 Shifts in methods of surveillance: Increasing possibilities of surveillance will induce more normalising effects on conduct, self-perception, personality, and world-view, than ever before.

3 Shifts in power relations: Regulation will be delegated more from persons to technology and from public, governmental parties to private organizations and citizens.

4 Changes in the governability of technologies themselves: Growing uncertainty and complexity will increasingly complicate the governance of the emerging technologies and their applications.

5 Shifts in privacy concerns: As new possibilities of observation and surveillance show both centralizing and decentralizing tendencies (that do not mutually neutralize each other) and instruments for observation and surveillance become increasingly unobtrusive, both the perception and the nature of privacy invasions will change.

6 Shifts in the focus of criminal law, away from reaction, retribution and rehabilitation, towards prevention and risk control.

7 Shifts in the conceptions of freedom and personal responsibility: These may affect the ways in which persons perceive their own and others' identities; they need not automatically undermine conceptions of morality and law that take personal responsibility and free will as their starting points.

8 Growing fusion of norms and enforcement: The inclusion of norms in technology that influences behaviour will involve increasing challenges to moral outlooks in which the free choice to act morally or legally right is primordial and new challenges regarding the legitimacy of arrangements for regulation and enforcement.

As the world changes and technology develops, normative outlooks can be expected to change as well. Some of these changes have been indicated in the description of the trends. It is nonetheless important to note that the trends could also be seen as explicating a necessary additional element in the scenarios. Impacts occur in context, and are co-produced through technological developments and social and normative developments.

Impact assessment has to take this into account, up to the further possibility of normative outlooks changing in the course of this co-evolution.

If the scenarios (and their background considerations) are combined with the present discussion of trends, key issues (and trends, and challenges) seem to be poly-centric governance, particularly in relation to infrastructures, the role of private actors in the new governance structures and self-control versus control by others. An important general challenge for the future will not be about government actors, but about the role of private actors and their accountability.

There is a general role of government vis-à-vis new and emerging technologies: to stimulate exploration and exploitation of new and emerging science and technology for what they can do and mean; but also to set boundaries to such developments because of possible negative impacts and the opening up of further, possibly undesirable applications. Here, co-evolution returns, now of technology, society and normative outlooks, including the expectations that norms and values might shift.

One should be very careful not to engage in an evaluation of the scenarios on the basis of the trends that were sketched. Nonetheless, in a kind of *addendum* to the report, the scenarios and the trends have been confronted with the principles and starting points that form the normative framework of the current Dutch criminal law system.

Eliciting the principles that lie at the heart of the Dutch constitutional state can help to assess the boundaries of the adoption of converging technologies for the purposes of monitoring people, improving forensic techniques, and profiling, identifying and monitoring potentially dangerous individuals or groups. These principles are not set in stone for eternity, however. They are co-evolving with the social and technical developments and with the changes in the relation between the interests of society at large and those of the individual. The inventory of principles and current (fundamental) rights merely clarifies where choices and trade-offs could be made.

1 Introduction

In this document we investigate the possible impact of converging technologies on practices of regulation and law enforcement. It is a forward looking study intended for practitioners and policy makers in the field of security, legislation, crime prevention, and law enforcement. We use three selected cases where converging technologies may fit in.

This study takes the technological developments as its starting point. We estimated what the developments in the field of converging technologies would be, mapped them out on the application domains mentioned and then set out to assess the trends in the social and normative impact of those developments.

1.1 What are Convergent Technologies?

Currently, the field of 'converging technologies' gets a great deal of scientific and public attention (Doorn, 2006; Schmidt, 2006; Silberglitt *et al*., 2006). During the debate some futuristic visions show up, including the idea of enhancing human performance (Roco and Bainbridge, 2002; Bainbridge and Roco, 2006). That is, we meet high expectations with respect to the application of converging technologies and their impact. But what exactly are converging technologies, how realistic are the expected technology developments, and what do they mean for a specific application domain, in our case the field of security, legislation, crime prevention, and law enforcement? This question has been the starting point of this study.

In general, four converging technologies are distinguished, namely nanotechnology, biotechnology, information technology (or ICT) and cognitive technologies (in short NBIC technologies)[1]. Of course more science and technology fields exist, but the NBIC technologies are expected to deeply influence application fields, are developing in a fast pace, and more and more influence each other. The NBIC technologies come closer to each other, leading to synergetic effects that accelerate the developments and supposedly lead to breakthroughs in all these fields. Therefore, one generally refers to these four technologies as *converging technologies*.

NBIC convergence fits in the information revolution and already exists. In IMEC's Human++ project (Gyselinckx *et al*., 2005), for example, key technologies and components for future wireless body area networks for health monitoring applications are developed. Prototypes aim at making EEG devices wearable in the sense of low-power wireless sensors, micro-power generation devices (using body temperature) and miniaturized processing unit (1 cm^3). This can be extended to entire body area networks (see Figure 3). This project focuses on brain signals (cognitive technology) but also deals with miniaturisation to make products wearable or to solve the energy problem (area of nano technology), with health care and the human body i.e. measurements on organic matter (relates to biotechnology) and in particular a lot of information processing (information technology). In interaction, these technologies result in artefacts and processes that could never have been obtained by applying the technologies individually.

[1] The term 'converging technologies' refers to both technology and science, e.g., nanotechnology and nanoscience, etc.

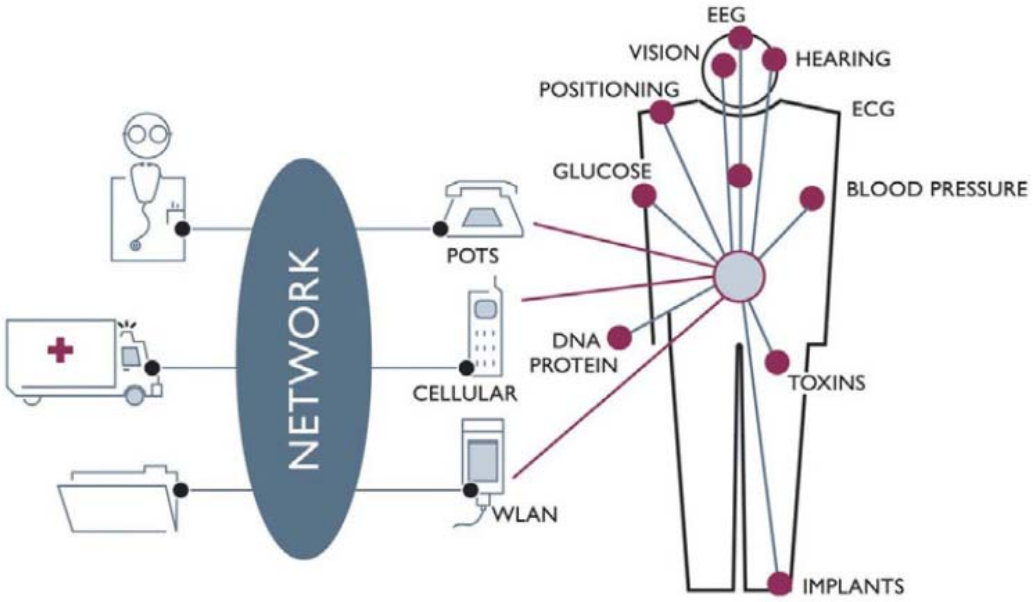


Figure 3: The technology vision for the year 2010[2]: people will be carrying their personal body area network and be connected with service providers regarding medical, lifestyle, assisted living, sports and entertainment functions (figure printed with permission from IMEC).

Many more examples can be provided, such as:

- Regenerative medicine: directed growth of bone cells[3] or neuronal tissue[4] on carbon nanotube scaffolding. Injecting molecules designed to self-assemble into nano-structure has been proposed as an alternative way of stimulating neural tissue growth.[5] It is an area where nano- and biotechnology meet each other.

- Lab-on-a-chip technology: small devices that allow a quick analysis for, e.g., medical or forensic research purposes. This development in nanotechnology may use biosensors and obviously relates to information processing.

- Gene chip micro-arrays integrate semiconductor fabrication techniques, solid phase chemistry, combinatorial chemistry, molecular biology, and robotics in a photolithographic manufacturing process that produces GeneChip arrays with millions of probes on a small glass chip[6].

- Direct implants (nano-wire arrays) that collect neural signals from individual neurons[7] can be further used to generate simple computer commands.

One critical point in a study on converging technologies is a proper definition of the field. The convergence is defined in Roco and Bainbridge (2002) as a 'synergistic combination of four major 'NBIC' (nano-bio-info-cogno) provinces of science and technology […].' The synergistic combination is indeed the key to understanding why

[2] Note that this 'future' vision of Gyselinckx et al. is close to realisation indeed.
[3] http://www.newsroom.ucr.edu/cgi-bin/display.cgi?id=1273
[4] http://www.sciencedaily.com/releases/2007/05/070520091842.htm
[5] http://www.nanotechnology.com/news/?id=10608
[6] http://www.affymetrix.com/technology/manufacturing/index.affx
[7] http://www.news.harvard.edu/gazette/2006/08.24/99-nanowire.html

and how convergence is different than a mere combination of two or more technologies. Rocco and Bainbridge proposed the nano, bio, info, and cognitive technologies as the key technologies that could contribute to improving human performance. In their view, these four technologies are converging in the sense that each could and should be used for modelling and solving parts of the complex problem of improving 'human abilities, societal outcomes, the nation's productivity, and the quality of life.' They coined the term convergent technologies to describe the interplay of these technologies in their future development. Nordmann (2004) defines this as follows: 'Converging technologies are enabling technologies and knowledge systems that enable each other in the pursuit of a common goal.' These definitions show that convergence is a means, not an objective, and mainly shows up in *applications* of technology.

According to the view of Roco and Bainbridge (2002), nano-science and nano-technology are the catalysts of convergence, since 'the building blocks of matter that are fundamental to all sciences originate at the nanoscale.[8]' From an ICT point of view, however, this last assertion is arguable and information technology will be claimed as being the 'glue' between all technologies. Convergence is therefore a process, and not a property of this collection of technologies. The NBIC technologies grow towards each other, which may result in new, additional technology fields that fuse the NBIC technologies together. Like in the ICT sector the technologies on telephony, internet and television (media) fused together. The main effect of the convergence processes is the achievement of reciprocal compatibility between the converging technologies.

Moreover, the individual fields of nano, bio, information and cognitive sciences are multidisciplinary as well. Take for instance the information technology, whose roots can (with a bit of imagination) be traced back to the musical boxes and mechanical calculators, to the Aristotelian 'tertium non datur', the Korean trigrams, and Boolean algebra, and to the macro-magnetism and triodes. However, these can only be related to modern computers in retrospect. From the perspective of, say, the mid 19th century (after the publication in 1854 of Boole's monograph 'The Laws of Thought'), the most daring mind could not have predicted the use of binary logic-based computers for playing 3D games, for finding your way in an unknown city, or for the creation of the Internet. Also, by definition the biotechnology combines disciplines like genetics, molecular biology, biochemistry, embryology and cell biology, which are in turn linked to practical disciplines like chemical engineering, information technology, forensics and robotics.

Consequently, in this document we first explore the developments of the four (multidisciplinary) NBIC fields of science and technology separately. Next, we address the new technologies resulting from the convergence of the four fields by sketching application scenarios in which convergence can be recognised.

1.2 Three objectives of this study

This study starts from a technology viewpoint. So the first objective of this document is to provide an initial assessment of the evolution, maturity, and perspectives of the nano, bio, information and cognitive technologies. Main attention is paid to the following questions:

[8] p. ix, op. cit.

1 Which are the most important scientific and technological breakthroughs that led to the current state of the four technology fields?

2 What is the current state of the art and which of the existing NBIC technologies are mature enough and relevant for our application field, i.e., will affect the constitutional state, legal order, and tasks of the Ministries of the Interior and Kingdom Relations and Justice?

3 What are the expected technology developments for the next 5 to 15 years, how realistic are these expectations and what are the main challenges?

Since answering these questions is an endless task, we expect that this literature scan will only provide a partial answer to these questions, and that some answers may still be affected by hypes (too high expectations) or counter-hypes (too high fears). For the purpose of this study, however, we do not want to forecast the future (as far as possible anyway) but only indicate the main developments in terms of feasibility and uncertainties regarding the development and convergence of the four NBIC fields.

The second objective of this study is to indicate the meaning of these technology developments for the policy areas related to regulation and enforcement. How can the government make use of these technologies? And what are the consequences for governmental tasks if third parties use these technologies? To delimit our scope, we focus on three specific cases:

1 Monitoring and following of objects and persons, and remote intervention in case of undesirable movements and relocations.

2 Improving and developing forensic trace analysis

3 Profiling, identifying and monitoring persons with an assumed security risk

Convergence of the NBIC technologies will show up in these applications. The time frame on which convergence will likely occur is estimated in the NSF report to be 2000-2020 (Roco and Bainbridge, 2002). Future scenarios of 5, 10, and 15 years ahead are therefore justified. For this reason, and because of the nature of some of the application areas – such as brain and behaviour influence – making a time horizon of 5 or 10 years would probably be too short, for our study a time horizon of 15 years has been chosen as well.

The third objective is an assessment of the social and normative, i.e., moral and legal impacts of the emergence of converging technologies in the application domains mentioned. New technologies offer new opportunities as well as risks with regard to regulation and enforcement. Insight into the choices and dilemmas which the progress in the convergence of NBIC technologies may make necessary is essential for our constitutional state. Therefore, this impact analysis is also part of this study.

1.3 Research approach

This research starts from a technology viewpoint: what are the developments and what is realistic for the next 15 years? Therefore, starting point is a state-of-the-art survey which has been based on a study of the literature and some interviews. In our attempt to give a technological view on the progress and perspectives of NBIC technologies and

convergence, we disregard at a first stage as far as possible the statements concerning societal, ethical, legislative and economical impact (be it beneficial or detrimental).

Our expectations for the coming 15 years have been discussed with an expert forum in two ways. First, a selected group of 16 experts responded on statements posed via a survey on Internet. Second, a group of 12 experts discussed in an expert session on the results of this web survey (the overlap between these groups was three persons). The experts are all either full professors or experts from a technology or application domain. Still reasoning from a technology point of view, we mapped the technology expectations on the application domain to investigate their meaning for the three selected cases. The central question being: what is realistic in 5-10-15 years with respect to the application of technology in these cases?

Convergence of NBIC technologies may lead to new technology areas or paradigm shifts in application fields. Paradigm shifts, however, can not be predicted in advance. Nonetheless, we want to sketch some examples of how convergence may appear in our application domain, in particular the three cases of monitoring, forensic research, and profiling and identification. To do so, we use a traditional scenario approach using certainties and uncertainties to identify a number of application domain scenarios (this approach is further explained and elaborated in Chapter 8). The resulting scenarios are a means to visualise the convergence of technologies for the application domain and herewith can be used as input for an impact analysis.

Only after the scenarios have been defined, we view the developments from other viewpoints besides the technology viewpoint only. The scenarios (and herewith the technology developments) are analysed from a moral, legal, and social viewpoint. In the context of this document it is impossible to study the moral, legal, and social impacts in depth. We focus on the main issues and again an expert session is used to discuss and validate the results.

Of course, in reality technology on the one hand and society and its normative outlook on the other hand, do not develop separately and in isolation. This study, therefore, should be looked upon as a thought experiment. The co-evolution of technology and society will, for the time being, be put aside. When the developments in technologies that can be used for surveillance, for instance, are sketched, possible limitations on those developments motivated by legal or moral privacy concerns will not be taken into account. The technological developments will be drawn as if merely motivated by internal dynamics itself. The possible social and normative impacts of those developments will be illustrated separately. In this way, the developments that may call for policy choices can be highlighted more clearly.

1.4 Reading guidelines

This document consists of three parts and a number of appendices. The first part, from Chapter 2 to Chapter 5, describes the state of the art and future expectations on nano-, bio-, ICT and cognitive science and technology, as well as their convergence. This part is independent of any application domain. Though it has been written to be accessible by a broad audience, parts of it may be very technological by nature. Seeking the balance between on the one hand describing a very broad technology field in a few pages, and on the other hand not being superficial, some professional jargon can not always be prevented.

The second part, from Chapter 7 to Chapter 8, describes the (future) applicability of converging technologies to our application domain, i.e., the acting field of the ministries who have commissioned this study. As requested, we focus on the three cases of monitoring and immediate action, forensic research and profiling and identification. Though the forecasts in this application part have been well-founded on the technology expectations of the first part, it can be read independently. This part ends with scenarios that are used as a means to 'visualize' the developments.

The third part, Chapter 9, is an impact analysis of the second part. The scenarios are analysed on their ethical, legal and social implications. This part describes the major social and normative trends we observe. In an addendum to this chapter, we also place these trends in the context of the current normative framework of the Dutch law. Obviously, this part frequently refers to the scenarios or technology developments, but nonetheless –for those readers who are e.g. mainly interested in legal issues– it has been written such that it can be read rather independently form the other parts.

2 Nanotechnology

Nanotechnology is a generic term that encompasses technologies that operate with entities, materials and systems of which at least one characteristic size dimension is between 1 and 100 nm. Often, the term also includes scientific research at the nanoscale. A common shorthand description of nanotechnology is: the study and manipulation of novel properties arising from matter on the nanoscale. A key aspect, also emphasized in the definition used in the US National Nanotechnology Initiative, is the occurrence of novel properties because of the nanoscale (e.g. large surface areas, quantum effects). Otherwise, large areas of physics, chemistry and molecular biology could be said to fall under the label nanotechnology.

Nanotechnology, as an umbrella term, contains various areas of emerging knowledge and innovative technologies, with different mixes of open/generic activities on the one hand and emerging linkages to other sciences, technologies and applications, and directions to follow on the other hand. In 'top-down' areas in nanotechnology, where micro-level phenomena and technologies are scaled down to nano-level (e.g. in lab-on-a-chip), there are often already linkages with application domains. In so-called 'bottom-up' areas where nano-level phenomena are the starting point (spintronics, nanotubes), the open and generic character is emphasised.

Nanotechnology is still at an early stage, which implies that it lives on promises (and disappointments) rather than actual performances. The overall promises of nanotechnology, such as nanoscale devices and tailor-made materials with specified performances, are programmatically translated in products and services, from better chemical and biological analysis to sun screeners to drug delivery. Although most of these products and services are still in infancy they create specific agendas for further development of nanotechnology.

Commonly, three main areas are distinguished:

- Nano-enabled materials and nano-structured surfaces
- Micro/nano-electronics
- Bionanotechnology and nanomedicine

In addition, there is instrument and technical infrastructure development (up to 'clean rooms'). And there is nanoscience, exploring phenomena at the nanoscale in their own right.

The transition from micro to nano is a continuum rather than a clear break (unless novel phenomena appear). This is definitely the case in the miniaturisation thrust in electronics. Starting at the other side, the bottom-up route, say when using quantum dots (a nano-particle that can programmably emit light), still the effects are realized in a micro-system. Nanotechnology enables better performance, and cannot realize this by itself.

2.1 Past breakthroughs

A brief overview (also drawing on an article in *The Economist*, March 2003) is shown in Table 1.

Table 1: Fundamental breakthroughs in nanotechnology.

1980 Binnig & Rohrer (IBM's Zürich Research Lab) file a patent for a 'scanning tunnelling microscope' (STM). Nobel Prize in 1986.
1984 Binnig invented the 'atomic force microscope' (AFM), which (like STM) also allowed manipulation of atoms.
1985+ Smalley, Curl and Kroto discovered carbon-60, or buckyball. Raised scientific interest (also more generally, in fullerenes). Both nicknames derived from Richard Buckminster Fuller, who invented geodesic domes of similar shape. Smalley got a Nobel Prize in 1996.
1986 Eric Drexler wrote Engines of Creation in which he posited miniature self-assembling machines ('and other fantastic notions' as The Economist phrased it), all linked to the term 'nanotechnology'.
1988 Three chemists at AT&T's Bell Labs showed that gold emitted light differently at the atomic level. 'That quantum-effect experiment is now seen as a landmark in the development of nanotechnology. It proved unequivocally that atoms behave differently from the way that classical physics would predict. But the researchers did not at the time think of it as nanotechnology.'
1990 'Then came nanotech's eureka moment. In 1990, Don Eigler, a researcher at IBM's Almaden Research Laboratory in San Jose, California, formed the IBM logo out of xenon atoms. A parlour trick, good for nothing practical. But it galvanised other scientists, who had never before seen atoms manipulated so completely.'
1990 Kratschmer (MPI Germany) and Huffman (Univ. Arizona): how to make buckyballs in large quantities, so that they could be studied properly.
1993 Iijima (NEC, Japan) and Bethune (IBM Almaden) discovered 'carbon nanotubes'.
1998 Giant Magneto-resistive (GMR) effect (1998) enabling dense hard-disk memories, and Tunnel Magneto-resistive (TMR) Effect (Moodera and Mathon, 1999) enabling dense solid state MRAM memories.
Late 1990s Supramolecular chemistry (Lehn, 1990) becomes involved: layers of oriented molecules, (supra-)molecular machines and molecular motors (cf. Browne and Feringa, 2006).

After the turn of the century, both nanoscience and nanotechnology expanded rapidly. From the many interesting new possibilities we mention just two examples.

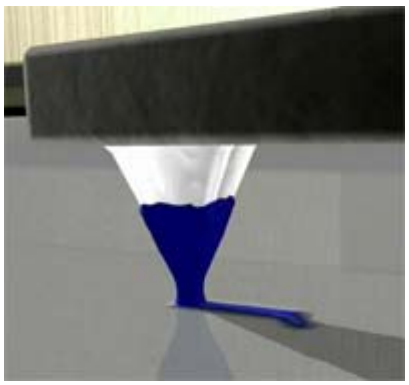


Figure 4: Dip pen nanolithography (by courtesy of NanoInk, Inc.[9]).

First, the active use of scanning probing instruments (rather than the passive scanning and imaging of the nanoscale). Tips can be used to make nano-pores in regular patterns, to create artificial membranes and sieves. Arrays of cantilevers can be used for fast analysis of compounds (including DNA) on a chip. Dip-pen nanolithography (see Figure 4) can be used for 'drawing' masks in the production of chips, particularly polymeric rather than silicon-based chips. (Semi-conducting polymers are the basis for various applications, especially so-called large-area electronics (system-on-a-foil), which are already used for low-performance tasks, but are seen as promising for a new generation of ambient intelligence.)

Second, the return of molecular assembly (Sun *et al*. 2000, Tripp *et al*. 2003). The notion of molecular assembly used to be associated with Eric Drexler's projection of the development of a 'universal assembler' capable of producing virtually anything out of individual atoms (Drexler, 2003a; Drexler 2003b). This projection has been criticized from the late 1990s onward, when nanotechnology came in for serious government funding (Smalley 2001, Smalley 2003a, and Smalley 2003b). The general opinion is that the original idea of a 'universal assembler' (and the attendant possibility of run-away nanobots turning the earth into Grey Goo) belong to the realm of speculation.

In the meantime, however, possibilities to manipulate at the molecular level, and to isolate and/or create molecular assemblies which can do work, have increased[10]. There is no way (yet) to turn this into macro-level effects, but there is a lot of interest, and visualisations are produced of molecular motors, and even a nano-car (Figure 5).

[9] http://www.nanoink.net/

[10] An intriguing example is the rotaxane molecular switch Rotaxane is a molecule with dumbbell-shaped component, made up of a slim section surrounded by a ring and ending in two stoppers. The molecule can act as a switch provided the ring can be induced to move from one side to the other side, and thus be the base of a storage device. Thus, there is a link with ICT. Availability for commercial use is expected around the year 2020. (http://news.softpedia.com/news/The-Molecular-Computer-by-2020-45346.shtml).

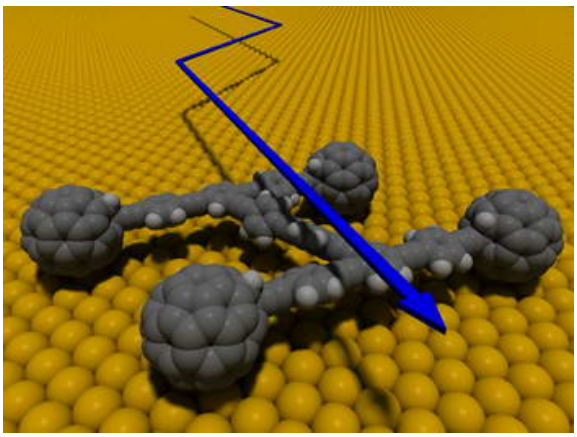


Figure 5: A 'nano-car' on a gold surface. (by courtesy of Y. Shirai/Rice University[11]).

2.2 State-of-the-Art

Nanotechnology covers many different technologies and developments. In the frame of this report, it is impossible to give a real overview. In addition, what is 'state-of-the-art' always includes an assessment of how present possibilities might evolve and deliver in the future. Thus, the notion of 'state of the art' is an ambiguous one.

Nano materials technology is currently the most mature of the nano-technologies and with the highest penetration in commercial products such as cosmetics, coatings, textiles, adhesives, catalysts, and reinforced materials. The mix of old and new is visible in the use of nano-clay particles to reinforce certain materials – which was done already, but now benefits from the better understanding of the effects.

Nano-electronics shows a mixture of ongoing improvements of established performance (as with hard disks and MRAM memories), nano-enabled developments (as in large-area electronics) which are ready for use but do not always have the right performance yet, and speculations based on new discoveries and proof-of-principle only. While 'Moore', i.e. developments in micro-electronics (specifically CMOS technologies) driven by expectations of ever higher performance as predicted by Moore's Law, has set the agenda for a long time, and continues to do so ('more Moore'), there is now a lot of work 'beyond Moore', with often uncertain prospects.

DNA micro arrays are available for fast throughput analysis, and lab-on-a-chip technology is in place, even if not taken up widely.

Sensors and actuators (MEMS/NEMS)[12] are an important growth area, in particular biosensors 'on the spot' which will replace taking of samples for measurement in laboratories (so-called 'point of care' analysis). Implants are being developed (improved cochlear implants, new retina implants). Nano-enabled precise brain stimulation is explored, and appears to offer positive effects, e.g. for patients with Parkinson's disease.

Nanotechnology enables the creation of biocompatible surfaces, important for implants and biomedical engineering.

[11] http://media.rice.edu/media/NewsBot.asp?MODE=VIEW&ID=7904

[12] Micro-Electro-Mechanical Systems (MEMS) is the integration of mechanical elements, sensors, actuators, and electronics on a common silicon substrate through microfabrication technology. Nano-Electro-Mechanical Systems include (enabling) nano technology.

Targeted drug delivery is an important promise, and various combinations of a drug (or active component) carrier (a nano-particle, a liposome), coated with functional groups which link to the target tissue (e.g. cancer cells), and ways of releasing the drug or inducing the effect (as when iron particles are to be heated by electromagnetic waves so as to kill cancer cells) are explored.

2.3 The next 15 years: opportunities, uncertainties, and challenges

There are many foresight exercises and more specific roadmaps for areas within nanotechnology. The International Technology Roadmap for Semiconductors, going back to the early 1990s, is now addressing 'beyond Moore' developments, and has to come to terms with the open-ended nature of these recent developments. While these are actively explored, they do not lend themselves yet to roadmapping exercises. In bionanotechnology, there is no earlier tradition. There are now ad-hoc exercises, and attempts, as by the European Technology Platform Nanomedicine, to create an overall strategic view. All these remain close to the state-of-the-art (cf. section 2.2).

The December 2003 Chemical Industry Roadmap for Nanomaterials By Design is interesting because it identifies the challenge of 'predictive understanding of structure-property relationships' so that nano-enabled materials can be designed to have desired performances. This will take 20 years, however. Within 15 years, rules for synthesis and assembly, based on understanding of 'chemistry' at the nanoscale will be available, as well as heuristics to create necessary building blocks, and to govern self-assembly. Earlier (5-10 years), high-throughput screening of trial-and-error designing of materials will allow efficient choices in practice.

An interesting attempt at an overall view is the four-generation scheme of Mihail Roco, senior adviser to the US National Nanotechnology Initiative (Renn and Roco, 2006; Roco, 2007a).

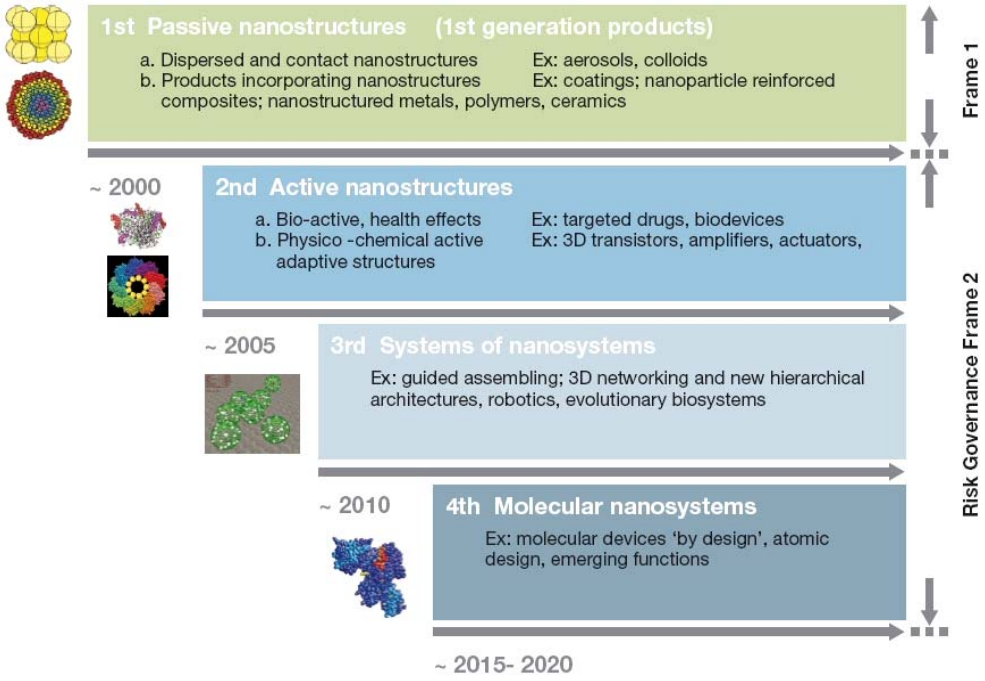


Figure 6: Timeline for beginning of industrial prototyping and nanotechnology commercialisation: Four overlapping generations of products and processes (by courtesy of Mihail Roco (2007a)).

The second generation, reactive ('smart') materials and structures, are capable to change their properties in response to different external changes (like temperature, electro-magnetic fields, humidity, etc.), and combine sensing and acting. The next step is to integrate some computing, so that choices can be made and acted upon. This is already visible in micro-systems, e.g. driver attendants that may block the driver switching to another lane on the highway. Nanotechnology will enable further functions and performances. Smart devices for the battlefield are being developed, and there is concern about the possibility of them getting out of control.

The challenge of assembly, how to aggregate what is possible at the nanoscale into performance at the macro-scale, is increasingly recognized (cf. Figure 7).

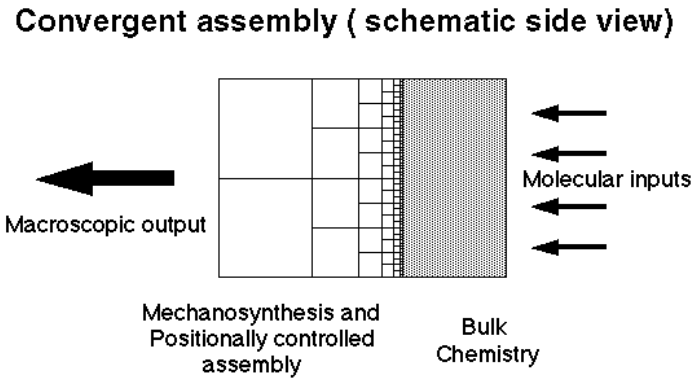


Figure 7: Convergent assembly of complex nanosystems (by courtesy of Ralph Merkle[13]).

[13] http://www.zyvex.com/nanotech/convergent.html

Another critical challenge is the evaluation of health and environmental risks, now particularly focused on nanoparticles. Concerns about these risks might block further development. This is recognized by nanotechnology promoters as well as by regulatory agencies, and research into such risks is promoted after earlier signals (e.g. Oberdörster, 2004) that there is indeed cause for concern. Current health and environmental risk regulation may not be sufficient because based on dosage in terms of weight or chemical composition, as nanoparticles have additional effects because of surface area and novel properties. This could be accommodated in the current regulation (including the upcoming EU REACH regulation) by taking nanoparticles, say of gold, as a new entity, rather than an instance of the macroscopic compound.

2.4 Discussion on nano technology developments

We posed our expert panel on Internet the following question: 'In what time frame are the following nano technologies mature enough to be applied in the security domain?'

– Reactive ('smart') materials capable to change their properties in response to different external changes (like temperature);

– Micro-chip technology with sub 10 nm structures of active components;

– Nano-manipulators for nano molecular assembly;

– Nano imaging tools for visualisation of nanoscale structures.'

The possible answers are within 5 years, within 10 years, within 15 years, more than 15 years, and no opinion. Figure 8 shows the answers of the experts who felt themselves confident to answer this question.

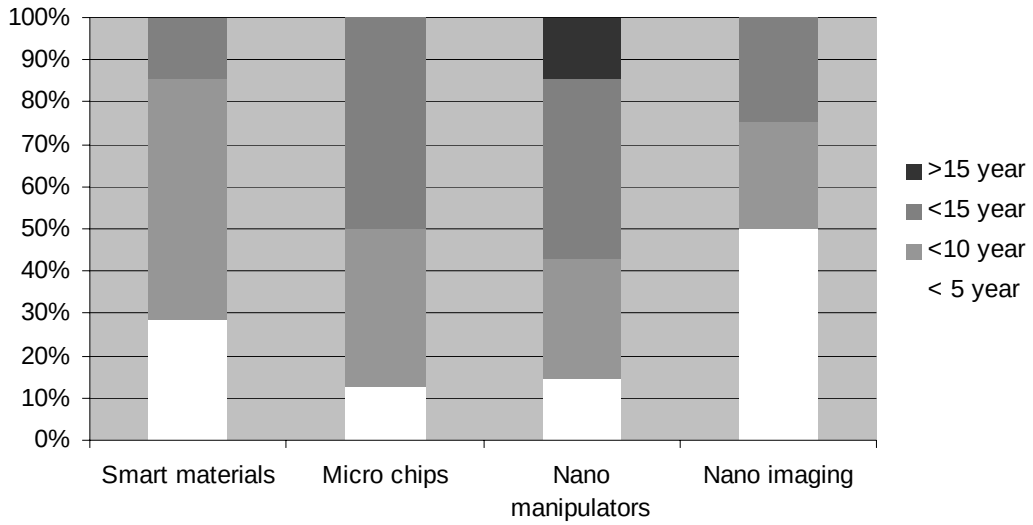


Figure 8: Expected applicability of nanotechnology in the security domain.

The expert opinion is that smart materials can be applied in 5-10 years, and microchips and nano manipulators in 10-15 years. The opinions on nano imaging diverge: half of the experts expects applicability within 5 years (earlier than for the other areas), while the other half expects applicability in 10-15 years.

Evaluating these opinions in an expert session emphasized that it takes a long time from lab to practical application. For example, it took at least 5 years to bring DNA analysis chips from a technological option to a technology that can be used by 'anyone'. For nanotechnologies like reactive smart materials, an even longer trajectory is expected. In the lab, many things already work. The conditions in a lab, however, are 'perfect' compared with the complexity of practices. Thus, the development of a device that works in practice takes a long time.

2.5 Conclusions

Nanoscience continues to be fascinating in its own right. Nanotechnology is an umbrella term covering a variety of technologies related only because their performance derives from nanoscale phenomena and manipulations. Thus, it is almost impossible to offer a comprehensive state-of-the-art and future prospects. The terminology is not settled either, so experts can respond differently to questions posed to them, depending on how they interpret key terms in the questions.

Sometimes, nanoscale phenomena have a direct application, as when quantum dots with controlled fluorescence are used to trace drugs or identify specific cells (e.g. cancer cells). In most current and near-term applications nanotechnology is an enabling technology which improves performance, and sometimes adds another performance dimension (as when nano-particles change the properties of sun screens).

Present and immediate future applications are visible in nano-enabled materials and surfaces, and in some nano-medicine applications (sensors, imaging). In further miniaturization in micro-electronics, the nanoscale is reached. In the exploration of the world 'beyond Moore', nanoscale phenomena are important, but they still have to be aggregated to deliver meso- and macro-functionalities. That aggregation step is one of the key challenges.

Still, an enabling technology may make a big difference, because it may lower thresholds for further functionalities. Radio-frequency identification devices (RFID) are a case in point. They will become smaller and cheaper, and can therefore be used more widely (to tag products, to be used in implants) and become a constitutive part of ambient intelligence and security infrastructure. In addition, they may get their own power, and so be able to send information, rather than wait to be read. Of course, the overall impact depends on the devices which are enabled by nanotechnology, and the systems of which the devices are a part.

3 Biotechnology

Biological technology is technology based on biology, the study of life. Before the 1970s, the term biotechnology has mainly been used in the food processing and agriculture industries. Since then, the term biotechnology is also used for engineering techniques related to the medicine field, like the engineering of recombinant DNA or tissue culture. Recombinant DNA is a form of artificial DNA which is engineered through the combination or insertion of one or more DNA strands. It includes the isolation, manipulation and reintroduction of DNA into cells, usually with the aim to introduce new characteristics ('genetic modification'). Tissue culture refers to the growth of tissues and/or cells separate from the organism. Nowadays, the term biotechnology is used in a much broader sense to describe the whole range of methods to manipulate organic matter to meet human needs.

OECD (2005) uses two definitions for biotechnology. First the single definition: *biotechnology is the application of (bio)science and technology to living or non-living materials for the production of knowledge, goods, and services.* Second a list-based definition that functions as an interpretative guideline to the single definition. The list is indicative rather than exhaustive and is expected to change over time as biotechnology activities evolve:

- DNA/RNA: Genomics, pharmacogenomics, gene probes, genetic engineering, DNA/RNA sequencing/synthesis/amplification, gene expression profiling, and use of antisense technology.

- Proteins and other molecules: Sequencing/synthesis/engineering of proteins and peptides (including large molecule hormones); improved delivery methods for large molecule drugs; proteomics, protein isolation and purification, signalling, identification of cell receptors.

- Cell and tissue culture and engineering: Cell/tissue culture, tissue engineering (including tissue scaffolds and biomedical engineering), cellular fusion, vaccine/immune stimulants, embryo manipulation.

- Process biotechnology techniques: Fermentation using bioreactors, bioprocessing, bioleaching, biopulping, biobleaching, biodesulphurisation, bioremediation, biofiltration and phytoremediation.

- Gene and RNA vectors: Gene therapy, viral vectors.

- Bioinformatics: Construction of databases on genomes, protein sequences; modelling complex biological processes, including systems biology.

- Nanobiotechnology: Applies the tools and processes of nano/microfabrication to build devices for studying biosystems and applications in drug delivery, diagnostics etc.

In their biotechnology trend analysis, the CBD/COGEM/Gezondheidsraad (2007) adds to this list biofuels, emerging diseases, vaccination issues, pre-birth and pre-implantation diagnostics, molecular diagnostics, large scale screening, diagnostic DNA research.

Biotechnology combines disciplines like genetics, molecular biology, biochemistry, embryology and cell biology, which are in turn linked to practical disciplines like chemical engineering, information technology, and robotics.

Since our target cases focus on monitoring and influencing people, in this section we mainly address bio engineering and life sciences applications.

3.1 Past breakthroughs

Biotechnology has a long history, but its present profile, also in relation to our question about converging technologies, emphasizes genetic manipulation and further ways of influencing processes in living organisms and profit from them.

In 1953 James D. Watson and Francis Crick elucidated the double helix structure of DNA based on earlier X-ray measurements of Rosalind Franklin. This proved to be a key factor to the understanding of the molecular mechanisms behind genetics and the working of the fundamental ACTG- genetic code for amino-acids in peptides.

From 1971 cell biology got an impulse with the signal hypothesis explaining the inner organisation and transport of cell secretes (Blobel and Sabatini, 1971) [14].

In 1982 the first transgenic mice were created. The micro-injection of genetic in vitro fertilisation allowed for specific selection and forms of embryonic cloning. From 1989 on these animals were engineered to produce blood or secretions (e.g. milk) with a certain concentration of a wanted protein with therapeutic value in human medicine.

In 1985 Peter Gill, Alec J. Jeffreys and David J. Werrett described new analyses of blood and semen samples in *Nature* (Gill *et al.*, 1985). This earliest method analysed the distribution of the hyper-variable mini-satellite regions (Jeffreys *et al.*, 1985a; Jeffreys *et al.*, 1985b). These segments in human DNA vary among individuals.

The discovery of the PCR (Polymerase Chain Reaction) technique by Kary Mullis in 1983 enabled exponential multiplication of minute amounts of DNA into manipulatable and analysable quantities. This allowed the technique of chemically cutting up DNA at known gene sequences and after PCR multiplication of the fragments and isolation to localise genes. The analysis of the characteristic distribution of fragments of a piece of DNA (DNA fingerprints) became also available for various application domains. DNA Fingerprinting methods turned to STR (Short Tandem Repeat patterns) analysis (Kimpton et *al.*, 1993) which, thanks to PCR can even be applied on the DNA of a single cell. STR analysis is now a well established technique. Fingerprints have become an important biometric to the field of forensic analysis.

In the 1980s breeding techniques for gene knockout animals were developed. The gene knock-out technique opened up the way to a better understanding and curing of genetic

[14] See also http://nobelprize.org/nobel_prizes/medicine/laureates/1999/press.html

diseases as well as understanding the working of the healthy organism by comparison to the knock-out alternative.

The first gene therapies, which are currently pioneered in human medicine, were conducted on mice successfully as early as 1990. Today we experience the dawn of the 'age of life sciences' where the knowledge from genetics, cell biology, etc., come together in new fields such as functional genomics, synthetic biology, proteomics, and gene therapy. In Table 2 we list some precursors.

Table 2: A selection of breakthroughs in biotechnology.

1973 Shih and Martin publish their General Method of Gene Isolation, a precursor of the PCR method.
1973 David Goldenberg demonstrated that radio-labelled antibodies against a human tumour antigen (CEA) could target and image human tumours in animals.
1975 Köhler, Milstein, and Jerne invent a technique to produce monoclonal antibodies
1982 Palmiter and colleagues create transgenic 'mighty mouse' with rat's growth hormone (Palmiter, 1982).
1985 Alec Jeffreys, Victoria Wilson and Swee Lay Thein show the first viable method for DNA fingerprinting based on mini-satellite regions offering a new forensic identification method.
1986 Kary Mullis addressed the Polymerase Chain Reaction for amplifying DNA strands which speeds up the biotechnology revolution with genetic fingerprints from small DNA samples and the human genome project as a result (Mullis et al., 1986).
1986 Steen Willadsen publishes the first successful technique for embryonic cloning, primarily proven to work on sheep embryos, but tested for a wide range of species soon after (Willadsen, 1986)..
1989 Behringer and colleagues show the principle of the animal as biological factory by synthesizing functional human haemoglobin in transgenic mice (Behringer, 1989).
1989 two independent teams publish techniques to breed for gene knock-out animals (Capecchi, 1989; Koller et al., 1989).
1990 Kyle and colleagues conduct gene therapy on mice to cure MPS (Kyle et al., 1990).
1992 Silva and colleagues show the use of 'knock out mice' to reveal the role of kinase II – a phosphorylisation enzyme – in the central nervous system to enable the long-term potentiation of neurotransmitter release, i.e. to enable long term memory function (Silva et al., 1992).
1996 Shoemaker and colleagues publish the gene chip to study functional genomics by the observation of the activity of genes in parallel rather than through gene knock-outs (Shoemaker et al., 1996).

1997 Scottish scientists report non-embryonic cloning of a sheep, using DNA from adult sheep cells.

2007 Stroes presents a successful clinical trial of gene therapy for LPL deficient patients (Stroes, 2007).

3.2 State-of-the-Art

If we follow the earlier definition of biotechnology, the application of biological organisms or parts thereof in industrial processes, fermentative processes to make bread, cheese, beer or wine are examples. Bioscience improved our understanding of these processes, and micro-organisms, plants, and animals can now be deployed in many areas as 'factories' for product used in:
- food (fermentation products);
- chemistry (bio-active substances in e.g. detergents);
- environment (decomposition of noxious substances);
- pharmaceuticals (production of medicines).

In the 1970s a breakthrough occurred in molecular biology, enabling the isolation, manipulation and use of genes. The dominant applications have been in agriculture, food sciences and medical area. Also, a great deal of money was poured into biotechnology with the hope that miracle drugs will appear. However, while biotechnology is indispensable to understand the molecular mechanisms behind many drugs a biotech revolution in the sense of production of new drugs by means of recombinant DNA techniques has not happened at large in the pharmaceutical sector. Even so, the example shows how a value chain can be changed due to technology 'hypes.' Fundamental and applied research have become less separated and there has been a shift from a few (pharmaceutical) industries dominating the market into an open innovation network including many small companies (see e.g. De Bruijn *et al*., 2004).

Biotechnology has developed far beyond seed improvement and genetically modified oats, rice, etc. Building on the science of genetics, and on the new possibilities to map genomes, we will come back to these developments, but first note another development, intervention in humans. This has drawn the interest of criminologists to look for medication and therapies from a systems biological, biochemical, neurobiological, or biopsychiatrical perspective. For example Robinson (2003) discusses how to 'improve' humans, with criminal tendencies in a system's approach relating cells and genes eventually to individual and group behaviour at various (interacting) levels of analysis. At each such level, risk factors for criminality can be identified:

- *cell* – genes: the role of genes traits related to criminality like impulsivity, ADHD, empathy, conscientiousness, or sensation-seeking (biochemistry);

- o*rgan* – brain: processes like (low) self-control being related to (partly heritable, upbringing-dependent) neurotransmitter/modulator serotonin (neurobiology);

- *organism* – personality: like risks of difficult socialization, sensation-seeking, resulting from (drug-induced) hypoactive autonomic nervous system (biology);

- *group* – family and peers: factors like family violence, familial antisocial behaviours, deviant peers, peer rejection (biosocial psychology);

– *community/organization*: e.g. socially and physically disorganized unsafe neighbourhood, available drugs (anthropology, social psychology);

– *whole society*: society levels social disorganization, social structure, class (sociology, economy).

In analogy to Robinson's approach, the interventions from biotechnology and bioscience could function at various aggregation levels:

– Medicines to speed up or slow down a biochemical reaction, including psycho-pharmaceutical medicines intervening in neurobiological processes.

– Interventions in genetic material (ranging from selective breeding of plants and transgenic animals to forms of gene therapy in humans).

3.3 The next 15 years: opportunities, uncertainties, and challenges

The 2007 Biotechnology Trend analysis (CBD/COGEM/Gezondheidsraad, 2007) foresees that contagious bacterial and viral diseases, both from exotic and local origin will (re)emerge in the Western world due to increased travel, deficient immunity, and strains resistant to antibiotics or antiviral medication. This will demand new forms of detection, genetic screening, vaccination, and treatment. Also new vaccines, diagnostics and therapies are in demand for autoimmune and inflammatory diseases and addictions that can lead to chronic diseases or cancer. For many of these emerging diseases few vaccines have been produced so far due to lack of funds. There is therefore a demand for cost efficient, well targeted vaccines, diagnostics, and medication with a short production time. Promising techniques for future vaccination are reverse genetics, genetically modified weakened viruses, reuse of characterizing proteins in easy-to-produce vaccines which are less pathogenic and can be used to vaccinate life stock, enabling differentiation of infected from vaccinated animals (DIVA). Another big trend is ethnicity as a factor in genetic diagnostics and genetic screening of newborns, and population in general. The role of ethnicity is taboo-laden in the Western world, even though for some treatments or prophylactic measures it scientifically makes sense to diversify based on hereditary predispositions. Finally, the Trend Report foresees a conflict between the ability to diagnose aptitude for certain diseases, while treatment is not yet possible. This will likely lead to ethical debates: people may go 'shopping' for DNA-based health diagnoses, whether government likes it or not.

In an interview microbiologist Wiel Hoekstra added some additional perspectives on future trends:

– Genetic analysis is likely to improve both with regard to accuracy, speed, and ease of operation. An example could be the implementation of gene passports. In case such technological developments will lead to debates concerning the privacy rights, the prospect of misuse and the appropriate countermeasures will be part of this development. Genetic profiling could lead to understanding the evolution of some diseases, and to better treatments.

– Synthetic biology and synthetic medicine may lead to developing agents with various functional abilities, such as preventing pathogens from entering the body, exploit pathogens' vulnerabilities, or enhance the immune response to new pathogens.

– Biomedical engineering will continue to advance in the direction of producing more complex artificially grown tissues, such as cartilage. Functional tissues (organs) will be the next step. However, it is still difficult to predict how successful this technology will be. Stem cell research, currently hampered by ethical and moral concerns, will likely take a different, less morally dubious approach, by using stem cells collected from adult humans, or even cultured.

Literature stresses the possibility of synthetic drugs that could be designed at molecular level, such that particular functional properties are enabled. Their interaction with the target biological system could be first simulated in order to evaluate the efficacy and safety of these new medicines.

Gene therapy, and generally the modification of human genes will continue to be a major research area. This can lead not only to more efficient treatment of some genetic diseases, but also to some applications (such as eugenics, or cloning).

In conclusion, the improved understanding of genetic and genomic processes, the rise of X-omics (genomics, proteomics, peptidomics), and further progress in the domain of biosynthesis toward synthetic biology will lead to new paradigms in healthcare, medication, and public health policies and public opinions.

3.4 Discussion on biotechnology developments

We posed our expert panel on Internet the following question: ‘How long does it take before the following bio technologies are mature enough to be applied in the security domain?’

– Accurate, fast and easy to use DNA analysis tools;

– Gene passports presenting a person's individual genome;

– Genetic profiling, which lead to understanding the evolution of some diseases, and to better treatments.

The possible answers are within 5 years, within 10 years, within 15 years, more than 15 years, and no opinion. Figure 9 shows the answers of the experts who felt themselves confident to answer this question.

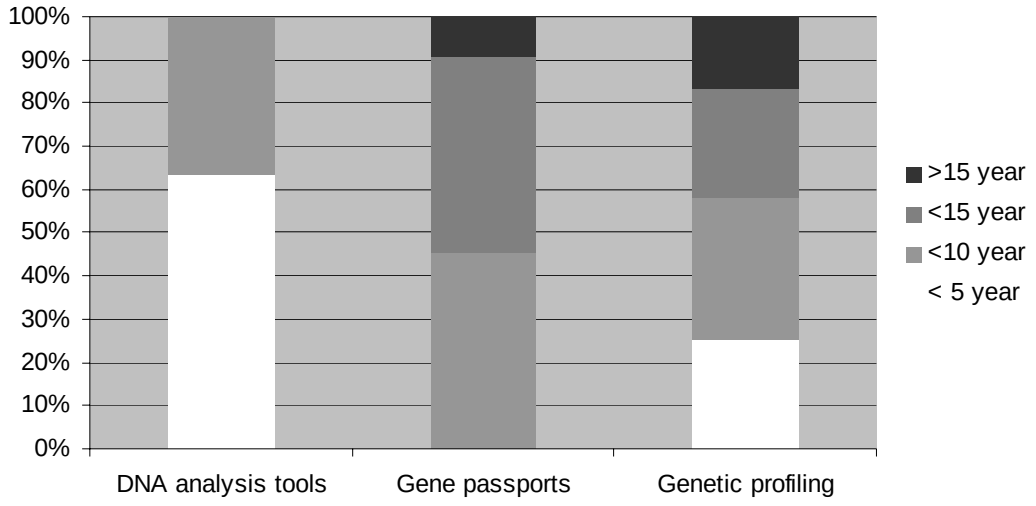


Figure 9: Expected applicability of biotechnology in the security domain.

The conclusion from Figure 9 is that DNA analysis tools are expected on the short term, gene passports are possible within 10-15 years, and the opinions on genetic profiling cover the entire spectrum from short to long term applicability. This variety in answers can be explained as follows.

Some genetic variations can be analysed very quickly. In this way, the sensitivity for some diseases like breast cancer can be determined. However, deriving a portrait or description of an individual based on someone's DNA is something far more complex. For example, during the case of the –by police and justice so-called– Meuse girl ('maasmeisje') forensic DNA analysis has shown that the victim should be of African origin. At first, this result shows the selectiveness of the analysis: still millions of persons match this profile. Secondly, the result of being able to extract this information is characterised as an exception, a stroke of luck.

Current technologies are able to produce the sequence of a mammalian-sized genome of the desired data quality for millions of dollars. The international objective is to reduce costs so that a mammalian-sized genome could be sequenced for approximately $1000 within 5 years. However, one of the issues is that the more we know, the more we see that in a complex organism like a human being only a part of the complex structure of phenotypical diversity lies in the structure of the DNA. A large part lies in the subtle mechanisms that govern gene expression, and the way gene expressions interact with each other and the environment. In addition gene expression is through peptides for which DNA determines the amino acid sequence but for whose function in the cell its three dimensional shape is of crucial importance, but very hard to predict with our current knowledge. This may explain why it is difficult to earn money from gene patents and, referring to changing value chains as exemplified in section 3.2, might lead to further changes in the balance of power within the value chain.

The extraction of identifying information such as portraits from genetic profiles is far away. Besides, there are some practical problems. Information like 'the colour of your eyes' is partly a matter of perception. Moreover, the smaller the volume of material, the larger the chance that the sample is contaminated. Nonetheless, this does not mean that genetic profiling can not be applied. Whereas legal proofs required a low margin of uncertainty, this is not always necessary in forensic practice. For example genetic

profiling could be used for investigative purposes where a higher level of uncertainty may be acceptable.

A quite other discussion that popped up during our workshop session (Appendix A.5) was the discussion on ‘business models.’ Many investments in ‘legacy systems’ have been done, which makes it difficult to replace existing practice. With current databases containing millions of DNA profiles of individuals with a criminal record, new profiling methods will not easily be adopted even if better technologies become available.

Finally, note that DNA is a complex matter. This raises the question whether there are not much more simple molecules that can be analysed for investigative purposes in stead of DNA. Biosensors specialised for these (within or on the body) may be of much more practical use for our application field.

3.5 Conclusions

The coming years, genetic analysis is likely to improve both with regard to accuracy, speed, and ease of operation. An example could be the implementation of gene passports. Also, synthetic biology and synthetic medicine may lead to developing agents with various functional abilities, such as preventing pathogens from entering the body, exploit pathogens’ vulnerabilities, or enhance the immune response to new pathogens. Biomedical engineering will continue to advance in the direction of producing more complex artificially grown tissues, such as cartilage. Gene therapy, and generally the modification of human genes will continue to be a major research area.

It is likely that biotechnology has an even greater impact on medicine as it has today. It might also become more important for food production despite resistance from consumers. Molecular genetics and biology will continue to develop and despite ethic problems there is likely to be increasing pressure to use, or misuse, genetic information about individuals. Gene therapy may be used in specialised medical treatment or as a form of doping in sports but is still in the research phase and in any case very much at the level of being able to produce a single enzyme rather than changing high level characteristics like behaviour.

In the field of forensics, DNA detection will become more sensitive needing less material, and distinguishing DNA samples will become more reliable. This will make large-scale databases that allow comparing DNA samples with DNA from the population more useful for forensic purposes, but while their creation requires no technical breakthroughs, it will require political will and funds. Once such a database is created, the ability to identify a person based on a DNA sample will be limited by the sampled data in the database, unless physical DNA samples are stored to redo analysis with future (or simply, more expensive) techniques.

DNA has proved its value for identification of a known subject. Using DNA for the extraction of identifying information –such as someone’s appearance– or to predict someone’s behaviour is a far more complex issue. This is as yet out of reach because besides the genotypical DNA structure, the larger context of complex processes in the living body plays a determining role. It raises the question whether simpler biological clues such as health or body functioning are available to understand behaviour.

4 Information Technology

Information technology encompasses all the technologies related to the logical and physical definition, design and implementation of systems and applications for data acquisition, storage, processing, transmission, and management.

4.1 Past breakthroughs

Just to set the scene we limit ourselves initially to the mainstream development of Information Technology. But embedded systems technology, radio frequency transmission technology and identification technology each have their scope of challenges, breakthroughs, and limits. Some of the most important moments in the ICT history are summarized in Table 3.

Table 3: Fundamental breakthroughs in information technology.

1887 Hollerith founds the Tabulating Machine Company, machines capable of sorting punched cards. Company later baptised as International Business Machines (IBM).
1900s -1940s several electromechanical computing devices show up.
1931 Kurt Gödel's Incompleteness Theorem shows that in any sufficiently rich axiomatic system that can handle arithmetic, there must be true propositions that are not provable within the system.
1936 Alonzo Church's lambda calculus and Emil Post's production systems, each of which, together with the following year's Turing machine, equivalently embodies the concept of effective computation as enunciated in Church's Thesis.
1942 electronic devices and algorithms developed to crack the enemy's secret codes
1945 Vannevar Bush publishes As We May Think foreseeing a worldwide hypertext not unlike the World Wide Web.
1945 completion of the ENIAC (Electronic Numerical Integrator and Computer), the world's first general purpose, electronic computer.
1948 Norbert Wiener writes about Cybernetics.
1948 Claude Shannon publishes his Mathematical Theory of Communication.
1950 Turing publishes Computing machinery and intelligence (Mind, Vol. LIX, No. 236, 433-460).
1952 the EDVAC (Electronic Discrete Variable Automatic Computer), using a stored program according to the Von Neumann architecture, starts operating.

1958 Jack Kilby's microcomputer chip.

1960-1968 Internet founder J.R. Licklider supervises the development of the NLS (oNLine System) publishes the Man Computer Symbiosis and the Computer as a Communication Device.

1965 Gordon Moore envisions that the nr of transistors on a chip increases exponentially over time (Moore's Law). Since then the nr of transistors has grown by a factor of 10^6 (see Figure 10)!

1971 Stephen A. Cook publishes 'The Complexity of the Theorem Proving Procedure' formalising the concept of NP-complete computational complexity

1973 Robert Metcalfe's local area network (LAN) Ethernet protocol.

1976 Cray I, the first supercomputer.

1983 massive information storage on optical compact disks CD enabling electronic publications.

1989 Tim Berners-Lee conceives of the World Wide Web and defines basic HTTP and HTML protocols.

1992 – present Digital 2G, 2½G and 3G cell phones with electronic services at one's fingertip.

1993 Leonard Adleman demonstrates DNA computing (molecular computing), using it to solve a small travelling salesman problem.

1993 Marc Andreessen leads team that develops Mosaic at the National Center for Supercomputer Applications igniting the Internet hype.

1994 – present Lots of Web-applications e.g. for brokerage, auctions, gaming, and social networks.

1997 IBM's Deep Blue beats reigning World Chess Champion, Garry Kasparov, in a full chess match.

1998 PhD candidates Brin & Page publish The Anatomy of a Large-Scale Hyper-textual Web Search Engine and build a company based on their ideas: Google.

1999 Photography turns digital when many cameras work with megapixel CCDs.

2000 Broadband network access available at home.

2001 USB solid state memory sticks render optical storage on CD obsolete.

2004 Tom Tom Go is the icon for GPS guided PDAs for location based services navigation.

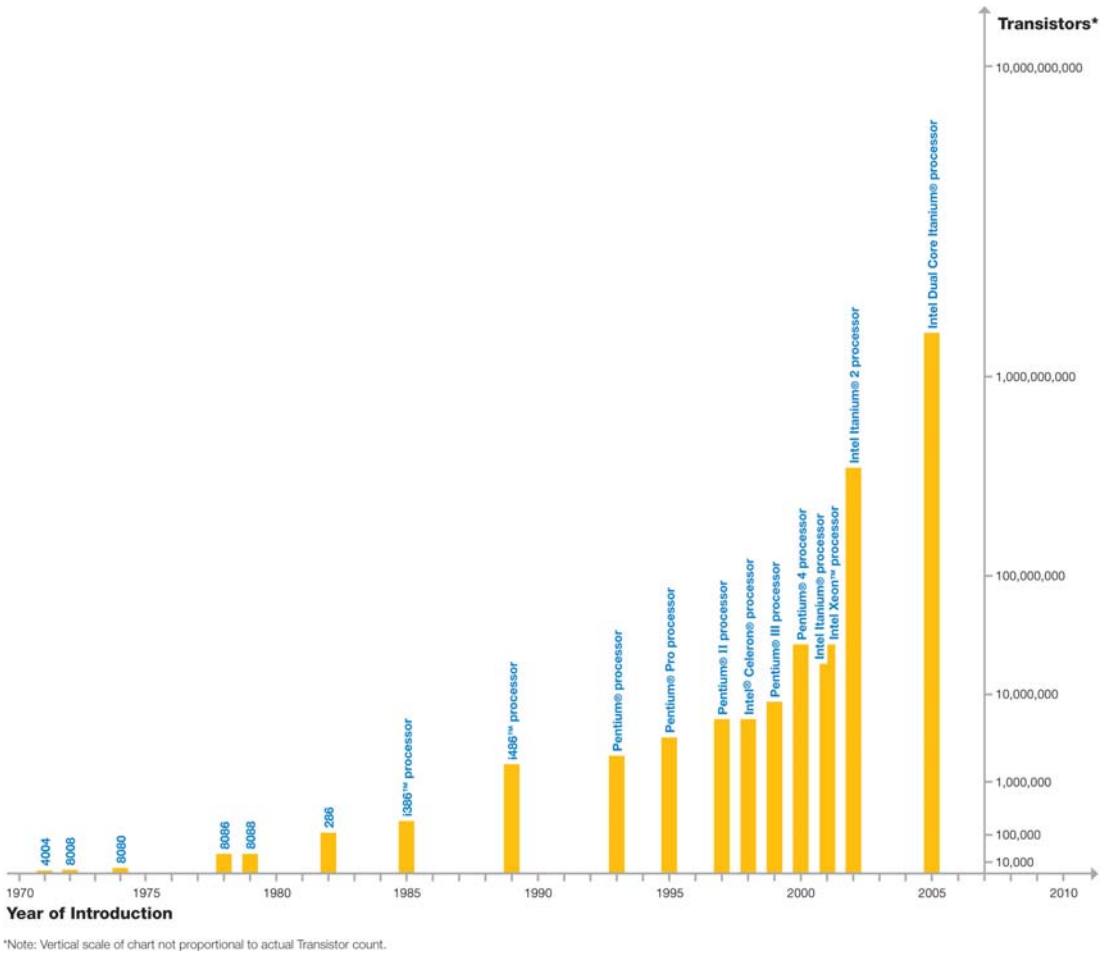


Figure 10: Processing power, measured in millions of instructions per second (MIPS), has steadily risen because of increased transistor counts[15] (Copyright © 2005 Intel Corporation.).

4.2 State-of-the-Art

Since almost all aspects of the current human activities heavily rely on ICT solutions (at least in the developed world), it is impossible to give a comprehensive view of all state-of-the-art applications. We present therefore a selection of those technological sub-fields that we considered most relevant for the current study and we address some issues posed to the field by other sciences. The developments in information technology are described using a categorization similar to the Reference Model for Open Systems Interconnection, commonly referred to as the OSI-model. We have simplified this model (4 instead of the original 7 layers) and distinguish between the physical, system, data and application layer of information technology.

Physical layer

– Processors: most relevant present day processors include general-purpose processors, RISC. Their computation power average around 20000 and 5000 MIPS, respectively at a clock speed of up to 5GHz. This clock speed cannot grow much further with given materials and architectures due to a trade off between speed and cooling[16].

[15] http://www.intel.com/technology/mooreslaw/
[16] J. Markoff, Intel runs into chip-making 'wall' and shifts strategy, *International Herald Tribune*, May 18, 2004

Innovation progresses via miniaturisation (45 nm gates in 2007), multi-core (parallel) architectures, new insulation techniques and eventually new substrates. Another category of processors includes programmable arrays and mixed signal processors for embedded systems.

– Storage: Space, speed, and reliability are no real issues any more (see Figure 11). Network storage is becoming common. Protected storage (e.g. smartcards, tamper-resistant hard-coded keys) are commonly used in commercial devices and applications. Nevertheless, all these properties combined with small size and low power consumptions are not yet available in commercial products. Technologies based on the Tunnelling Giant Magneto-resistance (T-GMR, see Moodera and Mathon, 1999) are now being developed to tackle these requirements.

Figure 11: Reducing storage sizes.

– Communications: wireless broadband over cellular networks and multi-megabit xDSL are widely deployed. Short-range communications (RFID, see Figure 12) enable completely new types of applications. Fibre optics is standard for core networks and starts being used for residential networks as well. Quantum communications is still in experimental phase, the latest results (June 2007[17]) showing that photons entanglement remains intact over a distance of 144 km through the atmosphere.

Figure 12: RFID chips become smaller and smaller.

– Sensors: small-sized, low-power sensors are currently available for most of the commonly occurring physical quantities: temperature, humidity, acceleration, pressure, superficial conductivity, magnetic induction, light (and other wavelength ranges). For special purposes such as forensic analysis complex sensors can be built e.g. for artificial smelling. They are described in the applications section.

[17] http://www.esa.int/esaCP/SEMXM7Q08ZE_index_0.html

– Actuators: besides the now classical electromechanical and electromagnetic types, new generations of actuators include: electrostatic, thermal, piezoelectric and magnetostrictive, constrictive dielectric (and generally electro-active) polymers (Mazzone *et al.*, 2003). Electro active polymers change their geometric properties (e.g. length) under an external electric field, being thus suitable for e.g. artificial 'muscles.' New research envisions the construction of actuators based on light-modulated Casimir force[18]. The field of sensors and actuators benefits largely from the developments in nano- and biotechnology. Another category of actuators include the visualisation devices. In this area nanotube-based fluorescent displays are currently being developed. 3D displays, and retina scanning devices are in a more advanced development phase, though still far from commercial-level maturity.

System layer

– Over the years different system architectures have been developed, starting with mainframe computers, networked workstations, stand alone personal computers, networked PCs and, with the advent of the Internet, distributed systems (grid computing, interoperable web services) for information services, and embedded systems for consumer devices. Also many ICT enabled devices and systems have been developed outside the computation realm such as mobile phones, digital cameras, home entertainment systems, and navigation devices. All of these tend to become more integrated within and across organisations.

– Network architectures: As for the networks, the connection to a central hub (whether it be a mainframe computer or today's home media server), gradually gives way to peer to peer networks and inter-networking. Bandwidth increases rapidly (see). In technical terms devices are increasingly multipurpose, enabling ad hoc wireless networking, multi-network interfaces and cross-network integration.

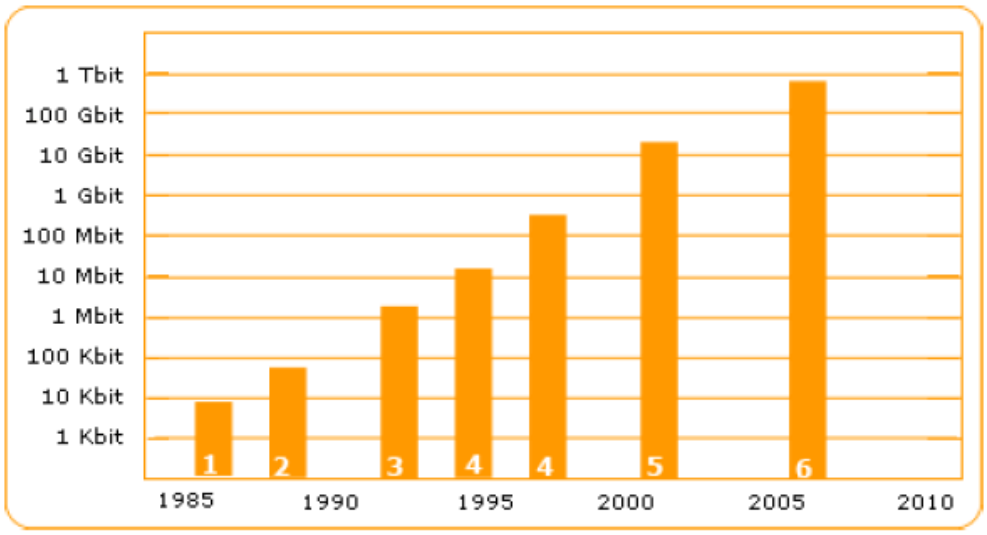


Figure 13: The transport capacity of SURFnet1 up to SURFnet6 (Dutch Internet infrastructure) has grown in an exponential way (by courtesy of Surfnet).

[18] cf. http://www.photonics.com/content/news/2007/June/1/87847.aspx

Data layer

- In the realm of data modelling, processing and analysis techniques, the main efforts encompass standards for cooperation, interoperability, usability, and presentation issues. The Semantic Web initiative is intended to add meaning to data, sophisticated user profiles are used for configuring the presentation layer of different applications and services, and Artificial Intelligence techniques are used for 'purposeful' analysis of large amounts of sensor data (video and audio). Data mining and pattern recognition are also widely used for intrusion detection, and even for signalling terrorism threats (Poindexter, 2002). Fields differ in maturity: A technique like speaker-dependent speech recognition is functional, while automatic recognition of some biometric features is not fully mature.

- Data compression and transmission techniques have developed remarkably thanks to the multimedia explosion: the theoretical limits for lossless compression have been approached, and the loss-making compression algorithms for audio/visual data already exploit all known limitations of human perception. Channel coding techniques, which enable efficient data transmission seem to have reached a physical limit by exploiting (e.g. in UMTS) the spectral, temporal and spatial division of channels.

- For the security of data and systems, and privacy the public key asymmetric cryptography can ensure almost any desired level of protection. Yet it is still not widely deployed due to the required infrastructural complexity. Commercial applications rely on simpler solutions, and reach a high level of protection through procedural, rather than technical means (e.g. token-based one-time-passwords). Digital Rights Management systems have seen an intense development effort, while its benefits are arguable. The latest Windows Vista includes DRM functions at the operating system level. Privacy enhancing technologies mainly rely on trusted third parties to hide the identities of interacting parties.

- Quantum computing, which was first suggested in 1982 by Richard Feynman[19] has already brought many new theoretical insights and practical achievements. Even though the first commercial company promises a 1024 qubit computer by 2008, it will probably still take 10 to 15 years before practical applications may be expected on a large scale. The stage of hardware development is promising[20], but challenges are manifold.

Application layer

- There is a current trend in computer applications to create ambient intelligence through smart, context aware surroundings, smart devices (e.g. automatic selection of washing programs based on the type and quantity of laundry or the pre-tension of seat belts when an impact seems imminent).

[19] Feynman, Richard (1982). Simulating physics with computers. *International Journal of Theoretical Physics* **21**: 467

[20] J. H. Plantenberg, P. C. de Groot, C. J. P. M. Harmans & J. E. Mooij Demonstration of controlled-NOT quantum gates on a pair of superconducting quantum bits *Nature* 447, 836-839 (14 June 2007)

– In the field of science support the main applications are computational science and e-science collaboration platforms. Computation co-develops with material science, cell biology, neuroscience, earth science, meteorology, and genomics (to name a few) where measurement data are exploding and new analytical and experimental paradigms are necessary.

– An unexpected but technically challenging class of applications stems from gaming and entertainment. In these domains new computer applications are being tested and developed that later on find their way into 'serious gaming' applications. Examples of these are robots as interactive toys, 'virtual worlds', and augmented reality environments. The latter also develops in professional applications (e.g. fighter pilots' helmet screens).

– A last big trend in computing applications comes from camera surveillance systems where the data explosion of an ever increasing sensor network calls for automatic recognition (identification or verification) of persons based on biometric features, and event detection as a form of pre-selection for human supervisors.

4.3 The next 15 years

The predictions for the next fifteen years are mainly based on Gorbis and Pescovitz (2006), Neild and Pearson (2005), the 2020 Science Roadmap Project conducted by Microsoft Research (2005), and Nature Magazine's special issue on the topic 'The Future of Computing' (23 March 2006).

Physical Layer

– Hardware innovation is happening at accelerated speed. Many of current trends will continue, while entirely new types of hardware will see the light. In the domain of networking a wide deployment of terabit optical core networks and gigabit residential networks is expected.

– Expectations with respect to quantum computing vary. Gorbis and Pescovitz expect the technology will not become commercially available within this time frame. But researchers like Andrew Steane, Chris Monroe, and Seth Lloyd (Nature, op cit. 398-401) emphasize that even small versions with a few dozen qubits could become meaningful e.g. for physics simulations. They may pave the way toward mainstream use in some distant future.

– There is optimism that miniaturisation will reach a near- to- atomic levels with processors with 5 nm gates becoming commercially viable. Also many developments in spintronics and Eproms suggest that non-volatile data storage will surpass RAM media. Electronic appliances of various kinds will be printable in functional polymers with desktop-printers. Finally 3D home printers are expected to become common.

– The face of computing will certainly change, while organic LEDs will be the dominant display technology; and foldable ultra light high contrast screens will be commercially viable.

– One of the big problems of today's portable applications is their energy consumption. It is expected that long lasting batteries based on fuel cells will be commercially-viable.

– As for small sensor network elements worn, implanted and spread about in rooms and offices, power-scavenging technologies will be integrated so that these sensor networks ('smart dust') and implantable devices stay functioning without battery replacement.

– One of the expected effects of the ongoing miniaturisation and robustness of technology will be body sensors to monitor blood flow and hormone level, and related to this, implantable drug dispensers (see also Figure 15).

Figure 14: System integration roadmap for the coming decade: the development of 3D stacking technology, flex technology, and full wafer-scale 3D integration will lead to 2 orders of magnitude reduction in volume and enable smart unobtrusive autonomous sensor systems (cf. Gyselinckx *et al.*, 2005; figure printed with permission from IMEC).

System layer

– Entirely new systems for e-science are to be expected. The sheer rise in volumes of acquired data, demand that computations are sent to the data instead of the current transmission of data forth and back.

– Also much more autonomy will be present in future systems. As far as dedicated systems for e-science are concerned, they support both autonomous and supervised operation.

– Users will collaborate in large tasks (be it scientific, policy making, or business). Grid like collaboration infrastructures need to become simple to use, as they may well become mainstream technology in everyday working.

– Systems are expected to become autonomous, maintenance-free, self-diagnosing and self-repairing systems to free users of time consuming activities.

– The same is true for networks which have to maintain their functioning in the event of a missing node, hence, resilient networks

– A large part of human computer interaction will be automated (and herewith 'become invisible') as smart tags (RFID-like) replacing bar codes will be integrated in many system functions.

Data layer

– The big challenges in future data storage, processing and management originate from its inherent growth. There will simply be too much data to transport coming from astrophysical, biological, medical, or chemical experiments. There will also be too much data to describe in natural language, and too much data to analyse in every detail. This means that data should be remotely accessible for computing, it should be easily accessible even in its vast amounts. Think of the current Google Earth as a sample service to interface access to large data quantities.

– As data will be an irreducible part of publications, it must be available for future generations as well.

– Data interoperability standards will emerge and will become an important quality of all data.

– Where interoperability standards cannot be defined, like in natural languages, universal translators will likely be developed. These will likely be available earlier than 20 years from now.

– Also human-machine interaction will be improved through recognition of handwriting and speech-based interfaces recognising unstructured speech with 99% accuracy.

Application layer

– Autonomy is a key feature in future applications. In the professional domain interesting new paradigms will see the light such as the chemical (or forensic, or biological, or physical) Turing machine. The very essence of laboratory work, including hypothesizing, analysing, and rejection/acceptance of a hypothesis, the optimal choice of experiments, will be outsourced largely to a hybrid computing system with experimenting capabilities. The current lab-on-a-chip gives a flavour of what future has in store. The role of the scientific or professional supervisor will lie in potential interventions in the functioning of the autonomous system, hence in creative decision making, visioning and focussing.

– In the general purpose market, authors expect a wide adoption of household robotics. This will also change the face of forensic operations. Robots can be used to photograph, sense, and sample a given area while not contaminating the evidence by the introduction of new footprints, fingerprints, or other human traces.

– Applications are expected that allow observers of large datasets some visualisation, 'experimentation', immersion, game-playing, tweaking and twisting. This will likely be done individually and in concert.

– The sensor networks will be spread around in the living body, in vitro in living cells, in the air to probe the atmosphere, or on earth to sniff, listen, film, etc. And the quality of the data collected, will allow better understanding of many complex systems. For these systems to be really understood, these experience interfaces need to be available.

4.4 Discussion on information technology developments

We posed our expert panel on Internet the following question: 'How long does it take before the following information technologies are mature enough to be applied in the security domain?'

– Quantum computing;

– Miniaturisation will reach a near- to- atomic levels with processors with 5 nm gates becoming commercially viable;

– Electronic appliances of various kinds will be printable on functional polymers with desktop-printers;

– Long lasting batteries based on fuel cells;

– Power-scavenging technologies integrated so that these sensor networks ('smart dust') and implantable devices stay functioning without battery replacement;

– Body sensors to monitor blood flow and hormone level, and related to this, implantable drug dispensers;

– Household robotics;

– New computing paradigms such as chemical, biological or physical Turing machines;

– Sensor networks spread around in the living body, in vitro in living cells, in the air.

The possible answers are within 5 years, within 10 years, within 15 years, more than 15 years, and no opinion. Figure 15 shows the answers of the experts who felt themselves confident to answer this question.

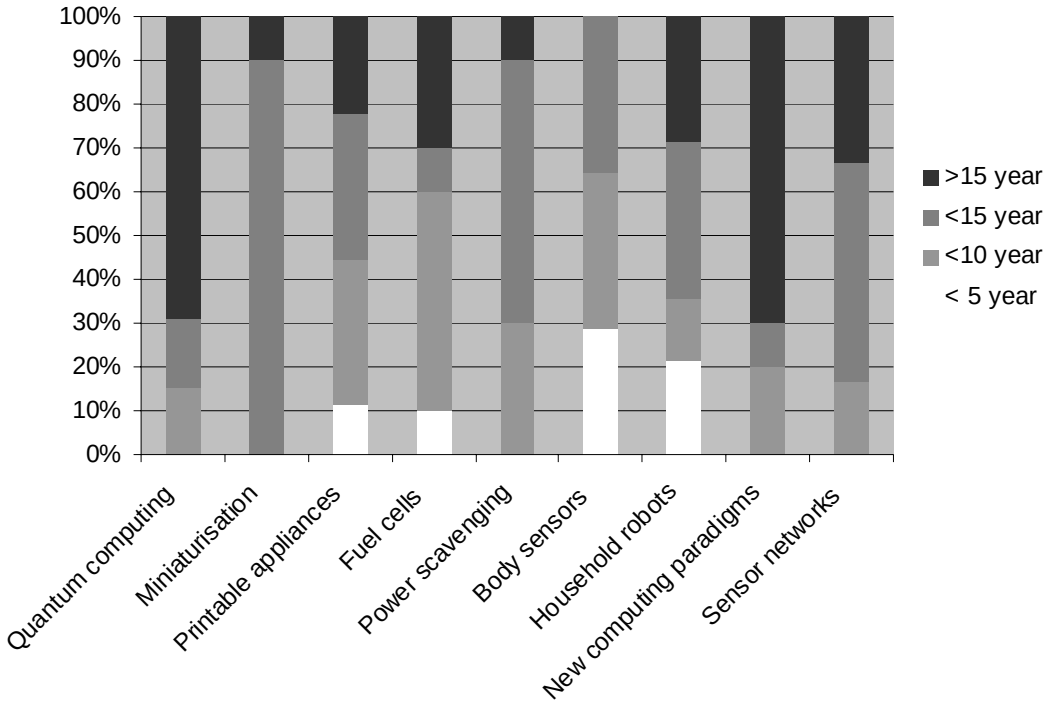


Figure 15: Expected applicability of information technology in the security domain.

From Figure 15 we observe that power scavenging and sensor networks in living bodies are expected in 10-15 years, miniaturisation of processors (almost unanimously) in a period of 15 years and new computing paradigms and quantum computing on the longer term, not within 15 years. On the issues of fuel cells, printable appliances, body sensors, and household robots, there is much more discussion on the period of applicability.

One of the bottlenecks in ICT may become the complexity of handling large volumes of data. For example, a single human genome as discussed in section 3 is already 6 Gigabit of data. This volume of data is still small compared with the possibilities of millions of RFID tags being scanned in logistic streams, the number of sensors growing enormously, and persons becoming continuously on-line with human-computer interfaces –due to sensors, speech technology, etc. – becoming more friendly. Quantum computing may be a solution for this problem, because quantum computing power is supposed to scale in an exponential way with the number of processors (whereas current computers scale in a linear way). However, quantum computers are judged as a long term development[21].

With respect to pattern and face recognition in video surveillance, the building blocks are available, but application in practice is difficult. For instance people have to be exactly in front of a camera to be identified. By conditioning circumstances, one may reduce the complexity of this problem.

[21] Computer scientist Leonid Levin criticises the quantum computing principle: 'Archimedes made a great dicovery that digital representation of numbers is exponentially more efficient than analog ones (piles of sand). Many subsequent devices have yielded unimpressive results. It is not clear why quantum computing should be an exception. In: The Tale of One Way Functions, *Problems of Information Transmission*, Vol 39, No 1. 2003, pp. 92-103.

Finally, another trend is the ‘web 2.0’, the entire development of people collaborating via the Internet and together working on something (‘social software’). This brings new economic models enabled by information technology. An application of these models may be the stronger participation of citizens in the security domain.

4.5 Conclusions

Innovations in information technology can be classified using the OSI-model into innovations in the physical, system, data, and application layer. In all layers major developments are to be expected in the years to come. Most striking developments for security enforcement are: quantum computing, miniaturisation on near-to-atomic levels, printable electronic appliances, power scavenging technologies integrated in sensor networks (smart dust), body sensors and implantable drug dispensers, household robots, new computing paradigms, and sensor networks spread around in the living body. Experts agree that an important bottleneck in information technology may become the complexity of handling large volumes of data. While an explosion of data is expected in many fields (e.g. data originating from astrophysical, biological, medical and chemical experiments) new computing paradigms and quantum computing are not expected within 15 years from now. Translated to the security domain this implies that detailed analysis of vast amounts of data on persons and goods will be an important challenge in the future.

5 Cognitive Sciences

For the purposes of this document the most relevant aspects of cognitive sciences are the study of structures, functions, and processes that define, implement, or describe the perception and interpretation of stimuli, decision making, and experiencing of mental states.

5.1 Past breakthroughs

Being an interdisciplinary field, the evolution of cognitive sciences is examined here from the perspective of psychology, neuroscience, philosophy, and artificial intelligence. Some of the most important moments in the ICT history are summarized in Table 4.

Table 4: Fundamental breakthroughs in cognition sciences.

1879 Wilhelm Wundt founded the first formal laboratory of Psychology at the University of Leipzig.
1886 Sigmund Freud began performing therapy in Vienna, marking the beginning of personality theory.
1895 Alfred Binet founded the first laboratory of psycho diagnosis.
1906 Ivan Pavlov published the first studies on Classical Conditioning.
1921 Otto Loewi discovers acetylcholine (Vagusstoff) as the first neurotransmitter (Loewi, 1921).
1932 Jean Piaget published 'The Moral Judgment of Children' beginning his popularity as the leading theorist in cognitive development.
1949 Donald Hebb hypothesized how memory traces would develop through repetitive coincidence of neuronal firing patterns (Hebb, 1949). This 'Hebb's law' of long term potentiation was later discovered in real in the rabbit's hippocampus by Terje Lømo in 1966 (Lømo 2003).
1953 B.F. Skinner outlined behavioural therapy, lending support for behavioural psychology via research in the literature.
1957 Leon Festinger proposed his theory of 'Cognitive Dissonance' and later became an influence figure in Social Psychology.
1958 Newell, Shaw, and Simon publish 'Elements of a Theory of Human Problem Solving' which was the first exposition of the information-processing approach in psychology.
1962 Electro physiologists David Hubel and Thorsten Wiesel presented their architecture how visual patterns were analysed by the mammal brain and mapped onto various brain regions (Hubel and Wiesel, 1962).

1966 J. J. Gibson publishes 'The senses considered as perceptual system,' on ecological psychology.

1967 Aaron Beck published a psychological model of depression suggesting that thoughts play a significant role in the development and maintenance of depression.

1977 Schank and Abelson publish 'Scripts, Plans, Goals and Understanding,' inspiring psycholinguistic experiments.

1980s computers play a larger role in psychological experiments, both for collecting the answers and for presenting passive or interactive stimuli.

1982 David Marr's 'Vision: a computational investigation into the human representation and processing of visual information.' Has been published posthumously.

1986 A. Paivio publishes Mental Representations: a dual code approach.

1990 George H. Bush declares the years 1990 as the Decade of the Brain.

1990 Nobel laureate Francis Crick together with Christof Koch set a research agenda for consciousness research, which to that date had been overlooked in brain research (Crick and Koch, 1990).

1993 Functional Magnetic Resonance Imaging (fMRI) became available for brain research and cognitive psychology.

1997 Deep Blue, the supercomputer at the time, beats the World's best chess player, Kasparov, marking a milestone in the development of artificial intelligence.

5.2 State-of-the-Art

The state-of-the-art of the field of cognition is presented from two perspectives: the theoretical models and empirical evidence explaining human cognition, and the design and implementation of artificial systems that display cognitive-like functions. The reason for this approach is emphasizing the synergy between these two major lines of research and development. On the one hand, explaining human cognition helps deriving architectures for artificial systems that implement some cognitive functions. On the other hand, developments in artificial intelligence can inspire new biologically-plausible models of human cognition.

Theories and evidence explaining human behaviour and cognition

The theories of human behaviour are as old as written history. As part of society's rationalisation during the nineteenth and twentieth century, scientific methods and theories were developed to explain and assess psychological wellness, and problems, and psychiatric disorders, to explain violence, crime, and to predict a worker's or soldier's, student's, or recruit's mentality, entry level, strengths and weaknesses. In retrospect many such theories seem oversimplified and even grossly unscientific. Yet the pioneers of that age paved the way for current methods to assess disorders, measure cognitive abilities, and assist in forensic analysis and rehabilitation practice.

As fundamental cognitive science focuses more and more on pure cognition, more 'practical' branches of psychology, psychiatry, and criminology have delivered a myriad of practical tools to test individuals, to treat several disorders through various forms of counselling and decide upon medication. Meanwhile a better understanding of the working of the brain has helped in the development of effective medicines for various disorders such as anxiety, depression, bipolar disorders and hyperactivity.

In this respect modern psychiatry combines both counselling and medication. For forensic science the spinoff of psychology's and psychiatry's development is twofold. One there are many tests that can be readily applied to select the appropriate 'treatment' for a given individual that has been convicted. The focus in criminology is shifting toward crime prevention. In that respect proactive rehabilitation of juvenile delinquents is promising. E.g., the Dutch project Halt stimulates young vandals to repair or compensate for the damage caused and improve their commitment to society. Two, the brain sciences provide methods to treat various disorders that often co-occur in delinquents. Doreleijers (1998) estimated that a quarter of all young criminals suffer from an undiagnosed ADHD disorder alone. Pelsser and Buitelaar (2002) have shown that dietary measures (less sugar!) can have a beneficiary effect here, while Gesch *et al.* (2002) showed an influence of several food supplements on juvenile delinquents.

For complex psychological or psychiatric disorders, the rare occurrence of disorders and the explanatory circumstances make it difficult to develop grand theories. Therefore, some psychiatric theories are still anecdotic in their evidence, just like in the days of Sigmund Freud. This does not mean however, that a person suffering from a 'complex' disorder cannot be assessed at all. Some brain scientists are confident that online measurement with fMRI will replace the polygraph (lie detector) as a system that cannot be fooled when arousal (and therefore the emotional reaction to certain stimuli) is at stake (see Figure 16). An fMRI scan would then be a safe method to decide on probational release. Yet, other brain scientist stress that this may not hold for psychopaths. They may just slip through the net because they can control their arousal system better than 'healthy' individuals. So, while some brain disorders may be detected precisely and early, many may be too complex to understand and analyse. Brain scientists generally agree that thought reading as such is next to impossible because of the complex interactions and activity patterns of the brain involved, so the classical ideal of a device detecting lies is a yet out of reach and will not be available as proof positive.

Advances in hardware and computing algorithms helped enable and improve noninvasive brain imaging techniques with a high spatial-temporal resolution. Maxwell's equations relating changes in electric fields to magnetic fields and vice versa are at work in these techniques. On the one extreme superconducting quantum interference devices (SQUIDs) enable recording minute magnetic fields (in the range of 1 femto (10^{-15}) Tesla) induced through neuronal currents in Magneto Encephalography with a millimetre spatial resolution and a temporal resolution comparable to intracranial electrodes (better than 1 ms). On the other extreme lies functional MRI which measures changes in cranial blood flow by 3D localisation of matter (and telling blood from brain tissue) by its nucleic spin alignment properties in response to a high (>1 Tesla magnetic field). The higher the magnetic field to which to align, the better the response and resolution. Improving magnetic field toward 7 Tesla enables fMRI imaging of the human brain with sub-millimeter spatial resolution and temporal resolution in the region of 125 ms (Pfeuffer *et al.*, 2002).

Obviously these improved brain imaging techniques will help discover, understand, and detect more of the brain's functioning and dysfunctioning. However, when applying these future insights to high level forensic phenomena such as 'violent intentions', 'criminal plans' or 'not telling the truth', their use might be limited. E.g., experiments by Mohamed *et al.* (2006) have shown that deceptive subjects tend to activate additional brain regions compared to truthful subjects. Yet, such tests may only work for untrained liars. The same argument goes for acts of violence. This could also be worthwhile for therapy and rehabilitation purposes. However, the proverbial cold blooded criminal may be difficult to identify by such tests, as the criminal habits have mingle into that person's ordinary behaviour. No significant difference may be found. Neither can such tests be turned around in all cases. A measured degree of empathy etc. might be alarmingly low, but then again: would someone with a lower than average degree of empathy necessarily have criminal habits? This problem cannot yet be solved.

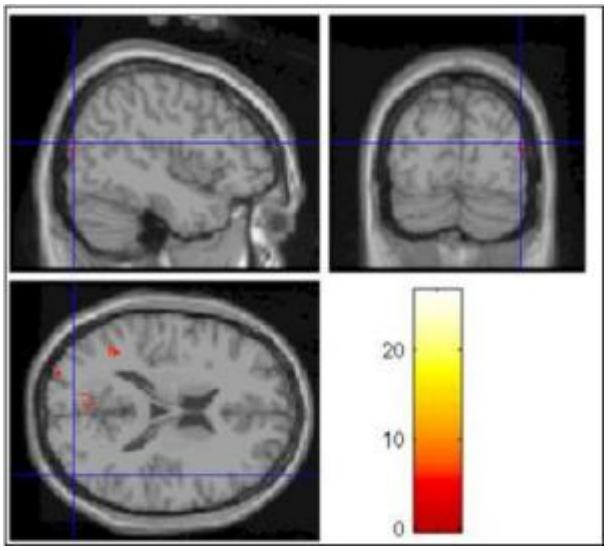


Figure 16: Lie Activation Temporal Lobe (by courtesy of Radiological Society of North America[22]).

The low hanging fruit in forensic science therefore might be much more in probabilistic methods that can be combined. For crime prevention, the individuals with a high risk might get extra attention and treat, and activities that might lead to criminal acts could be disturbed. While fMRI of the amygdale gives some insight in the emotions of an individual, so does the cortisol level which can be determined at low cost. Scientists agree that the future in behavioural understanding lies in combining methods from biology, psychology, psychiatry, and many social sciences.

The different theories of cognition cover only a limited number of aspects from all the processes and phenomena that pertain to cognition. The foundations of these theories are either based on empirical, physiological, or philosophical arguments. Their object is to explain either of the perception and action, knowledge acquisition and manipulation, or consciousness and mind. There is therefore no wide acceptance of one or the other of these theories, for which reason we choose to present a selection of some of the most representative ones.

From a methodological point of view, there can be identified two classes of theories. Computational theories of cognition propose mathematical or algorithmic description of

[22] http://www.rsna.org/media/pressreleases/pr_target.cfm?ID=206

neural processes. These theories are developed based on observed in vivo analysis of reactions to stimuli (e.g. through fMRI, EEG, etc.) and ex vivo analysis of neural structures. Empirical theories of cognition start from observed behaviours (or subjects' self-reports), and psychological assessments and propose models that logically explain the observed behaviours and psychological properties.

Computational theories tend to address lower-level (such as perception, recognition, or attention), and mid-level (concept acquisition, knowledge manipulation and management, decision making, etc.) cognitive processes. Most of the computational theories of cognition originate from the study of sensory and perceptual (especially vision), and motor processes. One of the most influential computational theories to date has been the three stage sketch model of visual perception developed by the late David Marr in collaboration with Tomaso Poggio (Marr, 1982). More detailed computational models start from the mathematical description of neural processes (either in individual neurons or in larger brain structures) to ensure in this way the biological plausibility of these models. A relevant example is the attention selection model proposed by Engel *et al*. (2001).

The theories concerning higher-level cognitive processes, such as mind states, experience, and consciousness are mostly empirical, and some quite speculative. Although full computational models for these high-level cognitive functions have not yet been developed, they would allow in principle a mathematical modelling, and ultimately an implementation in artificial systems. These are the so-called *identity theories of mind*, which hold that mind states are just properties that emerge from the chemical and electrical properties of brain states. Proponents of this stance (though with different nuances) are Smart (2007), Dennett (1991), and Pylyshyn (1984), to name only a few.

Dualist theories deny that sensations and thoughts are the product of electrical and chemical processes, and propose that the mind is of a different nature than neuronal states. A strong argument against the identity theory is the 'hard problem of consciousness' (Chalmers, 1996), which tries to explain the phenomenological experience. In Chalmers' view, only the 'easy problem of consciousness' (i.e. the ability to integrate information, discriminate patterns, attend and react to stimuli) can be explained by identity theories. The major difficulty the modern dualist theories encounter is explaining the mental states in terms of physical phenomena. Several attempts have been made in this respect, one of the most debated being the Orch-OR theory (see e.g. Penrose and Hameroff, 1996), which maintains that conscious states emerge as a result of quantum computations in synapses.

At the end of this paragraph we list some behavioural assessment methods, ways to treat disorders and act upon security risks that find their roots in cognitive science.

- Behavioural analysis (observation).
- Lie detection/polygraphy.
- Psychopharmacology.
- Behavioural therapy in juvenile affairs.
- Broadband methods: combining cognitive methods with biological methods.
- Facial expression (Paul Eckman's method).
- Cortisol level measurement.
- Psychological assessment (classical questionnaires).
- EEG tests, measuring arousal.
- fMRI tests measuring brain activity in relation to sensory stimulation.

Theories of artificial cognition

Theories of cognition that do not necessarily try to explain human cognition, or to account for observed brain processes have been developed for the purpose of implementing cognitive functions on artificial systems. For convenience, these theories will be referred to as *pragmatic theories of cognition*. Within the artificial intelligence (AI) field many analytic, logic, statistic, and algorithmic models have been proposed for learning, reasoning, categorization and clustering, pattern discovery and recognition, data correlation, etc.

Machine learning techniques attempt to devise mechanisms by which knowledge is acquired through experience. Depending on how the learning process is defined (that is the relation between the input data, the existing knowledge, and the feedback on how well the system performs at a given moment), several categories of learning techniques are commonly acknowledged: supervised, unsupervised, semi-supervised, reinforcement learning, and meta-learning (learning to learn). All these learning techniques produce a mapping (or association) between an input data pattern and a category label, much like humans learn the name of an object. The main properties these techniques should have are the *generalization* power – showing how well slightly different representation of the same input pattern are assigned one and the same label – and the *discrimination* power, showing how well the system can distinguish between different input patterns. Generally, the different learning algorithms can be designed such that either of the two properties is maximized, but a high-quality learning technique should optimize both. Nevertheless, even the best learning algorithms that only address these properties have limited utility in real-life applications.

More complex (and useful) properties are the ability of learning incrementally, i.e. to extend the knowledge set as new data is acquired. Although this seems trivial, it is quite difficult to implement in artificial systems. Several incremental learning algorithms have been proposed (see e.g. Polikar *et al*., 2001). Even more complex appears to be the learning of temporal patterns, namely not only labels of patterns, but also their evolution and interactions. Several architectures capable of implementing temporal learning have been proposed, one of the most debated at present being the hierarchical temporal memory architecture proposed by Hawkins and George (2006).

At a higher level, theories of selective and distributive attention have been proposed by e.g. Itti *et al*. (1998), Rasolzadeh *et al*. (2006), and Choi *et al*. (2004).

Currently, increasingly complex models mimicking high-level human cognitive functions are being researched in the fields of artificial autonomous agents, crisis response systems, and artificial consciousness. However, the current approaches in these areas still rely on the existing learning and reasoning techniques, for which reason the progress is rather slow. Several notable examples of complex cognitive architectures (combining many different cognitive functions) are the ACT-R (Adaptive Control of Thought--Rational; Anderson 1993) and SOAR (Symbolic Cognitive Architecture; Newell, 1990).

Next to mimicking the human brain in every detail, human brain functions can also be mimicked by software at a much more specialised level. The very application of software in decision support, pattern recognition, data mining, and pre-selection all boils down to some kind of smartness ‘in silico’. It may be a philosophical question whether the

algorithms developed have much in common with human or biological intelligent behaviour. Yet, few modern 'knowledge workers' would choose to work without computer assistance all the way. This assistance can be as simple as navigational or logistical planning in a pursuit or persecution. Location based data can be analysed to select those individuals that were close to a crime scene at a given time. In image analysis many new algorithms have been developed that identify with ease those pictures where a person or a certain object would be visible, thus reducing the time for human observers of camera systems. A microphone put at a scene can help identify situations where people are in real panic from situations where people just act panicked. The positive part of these developments is that artificial sensors can be extremely sensitive and widespread, while the computer algorithm can work 24/7. Compared to the human observer who can only be attentive for a few consecutive hours and whose sensorial system can only be attentive to one or a few details at a time, these artificial observation systems are an indispensable tool for crime prevention and security.

Yet, just like 100% brain reading is impossible, so will 100% artificial understanding of scenes and situations be improbable. This may be interesting from a theoretical perspective. For their practical applicability, this makes no difference.

Below we list some applications to understand human behaviour that stem from artificial methods, and likewise pattern recognition software.

- Aggression detection.
- Behavioural analysis (forms of terrorism).
- Forms of data mining (recognising complex behavioural patterns).
- 3D motion analysis / scene reconstruction.
- Artificial nose.
- Alcohol / drug tests.
- Expression detection.
- Body language detection.

Practice of investigation, evaluation and influencing cognitive functions and behaviour

In the previous paragraph the (im)possibility of understanding the human brain was discussed. Understand might help in crime prevention and in an improved evidence base for probational release. It does not help to 'cure' the disorderly brain.

Therefore, we address the practical side of influencing behaviour in this paragraph. Currently, a popular –but scientifically not undisputed– technique in practice is *neurofeedback (NFB),* also called neurotherapy, neurobiofeedback or EEG biofeedback (EEGBF). Neurofeedback[23] is a therapy technique that presents the user with real-time feedback on brainwave activity, as measured by electrodes on the scalp, typically in the form of a video display, sound or vibration. The aim is to enable conscious control of brainwave activity. If brain activity changes in the direction desired by the therapist, a positive 'reward' feedback is given to the individual, and if it regresses, either a negative feedback or no feedback is given (depending on the protocol). Rewards can be as simple as a change in pitch of a tone or as complex as a certain type of movement of a character in a video game.

[23] See e.g. http://en.wikipedia.org/wiki/Neuro_feedback

A method which seems very promising is Transcranial Magnetic Stimulation (TMS). This method stimulates the electrical activity in the brain at certain spots. The method works primarily on shallow brain regions close to the skull and it has proven effective in the treatment of some forms of depression. The interesting question of course is whether the changed electrical activity in these brain regions will persist over time so that a 'learning effect' has occurred. If this is the case, transcranial magnetic stimulation may be an effective alternative to some psychopharmacology or brain surgeries.

More drastic than TMS, in neurotechnology is *deep brain stimulation (DBS)*[24] . This is a surgical treatment involving the implantation of a medical device called a brain pacemaker, which sends electrical impulses to specific parts of the brain. DBS has been used for the treatment of some diseases like for essential tremor, Parkinson's disease, or to alleviate symptoms in treatment-resistant clinical depression. While DBS is helpful for some patients, its use is partly experimental and there is potential for serious complications and side effects. On the other hand, this technique does not destroy any brain tissue and can be turned on and off on demand.

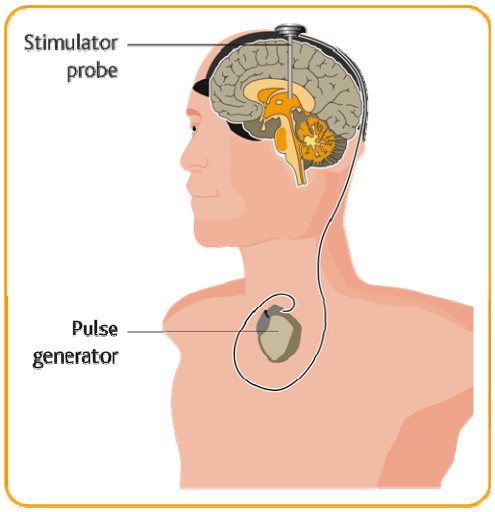


Figure 17: Deep Brain Stimulation is used for Parkinson's disease. It involves implanting wires into the specific areas of the brain that are overactive. These wires are connected to a device implanted under the skin on the chest that delivers electrical pulses, which are sent to the corresponding overactive areas of the brain to reduce their activity (by courtesy of Medtronic[25]).

5.3 The next 15 years

Futurists believe in the unravelling the secrets of human cognition and consciousness before 2020, but cognitive scientists are more sceptical. It is unlikely that the high-level cognitive functions (such as intentions formation, creative problem solving, and consciousness) will be fully explained.

Understanding the intimate relation between neural processes (either 'normal', or 'altered' through drugs or illnesses), and the conscious experience is rather unlikely. Nevertheless, it is possible to find a number of relevant correlations between brain states and mental states, which would allow some predictions of mental states from neural processes.

[24] See also http://en.wikipedia.org/wiki/Deep_brain_stimulation
[25] http://www.epda.eu.com/patientGuide/LWP_2_09_Surgery.shtm

Reading emotions from facial expressions is likely to become accurate enough for using in a wide range of applications.

With respect to computational models of human perception: although partial models of human perception are available today, not all perceptual functions are yet fully explained in a unitary way. It is likely that within 15 years a full model of perceptual functions will be available. To study information processing in the nervous system, physiological, anatomical and computational approaches can be used. The parts of the brain dealing with lower order functions, like the human and primate visual systems (how do we see form, color, shape etc.), can be identified. However, the modeling of higher order functions, such as visual semantics and consciousness will define the research agenda for the upcoming decades (25 years).

With respect to the synergy between brain and machines: some scientists believe not only that brain-machine interfaces will extend our senses, but also that memories could be uploaded onto computers, and thoughts could be communicated through direct brain links. However, thoughts and memories will be impossible to map on data structures before having a computational model of the higher-level consciousness. So the latter predictions seem beyond the likely evolutions for the next 15 years.

5.4 Discussion on cognitive science developments

We posed our expert panel on Internet the following question: ‘How long before the following cognition technologies are mature enough to be applied in the security domain?’

- Computational models of human perception;
- Reading intentions from facial expressions and micro movements;
- Contextual models of aggression;
- Early warning systems for behavioural derailing;
- Understanding the relation between neural processes (either "normal", or "altered" through drugs or illness), and the conscious experience.

The possible answers are within 5 years, within 10 years, within 15 years, more than 15 years, and no opinion. Figure 18 shows the answers of the experts who felt themselves confident to answer this question.

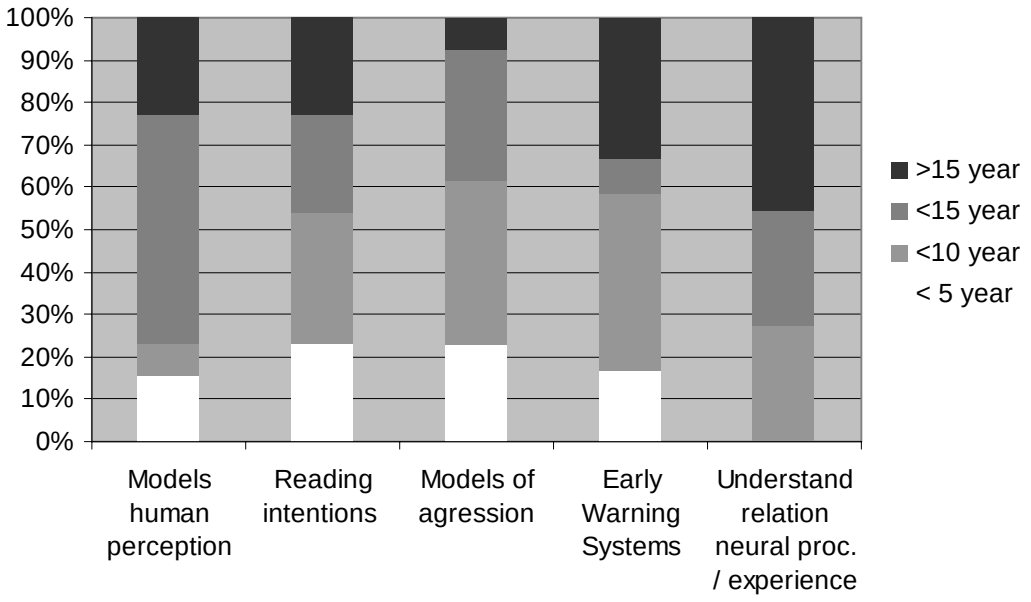


Figure 18: Expected applicability of cognition sciences in the security domain.

From Figure 18 we observe that contextual models of aggression may be applicable within 10-15 years. A computational model of human perception, however, is a long term issue. The term for applicability of reading intentions, early warning systems and understanding the relation between neural processes and the conscious experience is disputed. The discussion in our expert workshop shows the same line of thought. All issues mentioned are already happening! However, applicability in practice is another issue, and much more complex.

Finally, can we read thoughts in the future? As already indicated in Section 5.3, the brains are very complex to model. Experiments show that giving persons a task in an experimental setting, and on-line registering their brain activity shows that 40 times doing the same handling gives 40 different images, whereas looking to the same handling on television may give identical pictures. So there is a lot of noise. The general opinion is that 'brain reading' is over exaggerated. Of course, techniques like fMRI and EEG are very valuable for pathological purposes, with patients having clear deviations in their brain activity.

Identically, our forum is critical about selectively erasing memories. Moreover, experiments show that traumatic experiences –which should be erased? – are remembered very well, i.e., the best of all experiences.

Nonetheless, in the cognitive area there seems to be a lot of 'low-hanging fruit' to be applied for security purposes. EEG is a simpler and less expensive technique compared with fMRI. Probably much more can be done with facial expressions. We know very much about emotions. This knowledge seems to be applicable on the short term.

5.5 Conclusions

Brains are complex to model. Although futurists believe in unravelling the secrets of human cognition and consciousness before 2020, cognitive scientists are more sceptical. It is unlikely that the high-level cognitive functions (such as intentions formation,

creative problem solving, and consciousness) will be fully explained. Understanding the intimate relation between neural processes (either 'normal', or 'altered' through drugs or illnesses), and the conscious experience is deemed rather unlikely. Nevertheless, it is possible to find a number of relevant correlations between brain states and mental states, which would allow some predictions of mental states from neural processes. Nonetheless, in the cognitive area there seems to be a lot of 'low-hanging fruit' to be applied for security purposes. EEG is a simpler and less expensive technique compared with fMRI. Reading emotions from facial expressions is likely to become accurate enough for using in a wide range of applications.

6 NBIC convergence

In the previous chapters, we stressed that the science and technology fields of nano, bio, ICT and cognition are each multidisciplinary areas, combining several disciplines. Actually, the abbreviation ICT already reflects some kind of convergence. The fields of telecommunication (telephony), information technology (Internet) and media (television) merged into a new field in which we, e.g., make a call or watch television using Internet. As Van Est *et al*. (2006) state it, 'NBIC convergence fits in the information revolution, and is the most modern manifestation of this.' In this chapter we pay some more attention on how NBIC technologies are likely to converge in an evolutionary way. We give several examples of convergence because convergence shows up in applications. Also, we denote the direction into which we expect further convergence.

> *'Convergence is certainly a media term. Triple play is one example of such convergence. The newest cell phone sets can do Internet, text messaging, video streaming, and phone calls. And this is called convergence even when the underlying technology is the same.'*
>
> *Interview with prof.dr. John Long (TU Delft)*

6.1 Examples of convergence in existing technologies

In the next subsections we highlight several examples of convergence that indicate the current trends in this process. The list of examples is not exhaustive; neither do we want to mark these examples as more important as other examples that have not been mentioned. The examples listed, however, are held up as a typical model for the process of convergence, which shows up through the example applications.

6.1.1 Convergence between bio- and nanotechnologies

Previous chapters already mentioned some current examples of the convergence between bio- and nanotechnology, like regenerative medicine, lab-on-a-chip, micro array gene chips. Other examples are:

- Medicine: engineered cells (bacterially-derived) can transport chemotherapy drugs directly to cancer cells. Via antibodies on their surface, these nano cells latch on cancer cells, then are engulfed by these. Once inside, they release the drug. Test on humans are planned for late 2007[26] (Australian firm EnGeneIC).

- Active nanoscale devices: bacterial flagella can be used for propelling nanoscale artificial structures. The flagella motion can be switched on and off with particular chemicals.

- Transgenic food: food production by genetic manipulation.

The convergence of bio- and nanotechnology can be viewed from two perspectives. On the one hand, developments in nanotechnology are applied to biology. In particular,

[26] http://www.cancercell.org/content/article/abstract?uid=PIIS1535610807000906

biological systems can be measured or manipulated at the 'nano level'. Biosensors are an example: the sensors are fabricated using nanotechnology but use living materials (cells, micro organisms) as detector. On the other hand, biotechnology brings concepts like 'self assembly' to nanotechnology. Also, in nanotechnology living materials can be used as 'factory' or 'building block'. An example of the latter case may be the synthetic biology (see textbox). Finally, notice that in reality more than the two technologies (i.e. bio and nano) only may be involved. The bionanosensors are already an example of integrating nano-, bio- and information technology.

'Synthetic biology is another promising direction in biology that I expect to flourish. In 1973 researchers first showed that it is possible to produce hormones synthetically by using organisms as factories. In this so called recombinant DNA technology extra genes are inserted into an organism's genome that set the organism to making simple peptide hormones such as insulin in 1978. Currently biotechnology based on recombinant DNA technology is able of adding one or two genes to an organism's genetic makeup. More complex products cannot be produced with the same recombinant DNA technology. This is where synthetic biology makes the difference.
In synthetic biology the knowledge of DNA structure and functioning is used to make entirely new DNA constructs. In the future it is expected that entirely new pathways for protein synthesis will be constructed. Thus organisms will be developed that produce very complex proteins for various application domains such as medicine. […]
Researchers in synthetic biology basically take small micro-organisms such as yeast cells or bacteria. They strip these organisms to the point that they only contain what it takes to enable cell division and thus multiplication. The next step is to insert very complex recipes in that stripped genome. This way they develop an organism that produces, as though it were a chemical factory, very specific proteins. Such newly developed organisms are conceived via the drawing table. In that respect synthetic biology is as much a form of engineering as it is part of life sciences.'

Interview with prof.dr. Wiel Hoekstra (KNAW)

6.1.2 Convergence between cognitive sciences and ICT

Examples of convergence between cognitive sciences and ICT show up in the area of so-called 'brain-computer' interfaces. In section 5.2 we already mentioned the use of *deep brain stimulation* to control e.g. Parkinson's disease. Other examples are:

- In vitro development of neural circuits by stimulating a cell culture of brain cells. Through appropriate feedback the artificially grown neural circuit operates independently a flight simulator[27].

- Prostheses appear that substitute a body function. The current state of the art is e.g. arm muscles controlling an artificial hand and hence enabling mind controlled operation (see Figure 19, showing a commercially available bionic hand[28]).

[27] http://www.newscientist.com/article.ns?id=dn6573
[28] http://www.touchbionics.com/

Figure 19: The hand is controlled by the user's mind and muscles (by courtesy of Touch Bionics).

– The use of prostheses 'to replace or restore lost motor functions in paralyzed humans by routing movement-related signals from the brain, around damaged parts of the nervous system, to external effectors'. A *Nature* article (Hochberg *et al.*, 2006) describes a young paralyzed man who was fitted with a sensor chip designed to translate the electrical impulses from his thoughts into commands to a computer that controlled devices, such as an artificial limb[29].

Another area where information technology and cognitive sciences come together is the measurement on and modelling of cognitive systems, e.g. the prediction of behaviour and actions through brain scans. Examples of techniques are:

– FMRI: 70% success rate in predicting whether the subjects will add or subtract two numbers showed on a screen. Experiments also led to concluding that intentions are not encoded in single neurons, but rather in spatial patterns of neural activity.[30]

– ERP (Evoked Response Potential): ERP brain 'waves' (measured as potentials on different points on the scalp) following an acoustic stimulus indicate with high accuracy some neurological disorders, such as Alzheimer's, schizophrenia, dyslexia, depression (see Figure 20).[31]

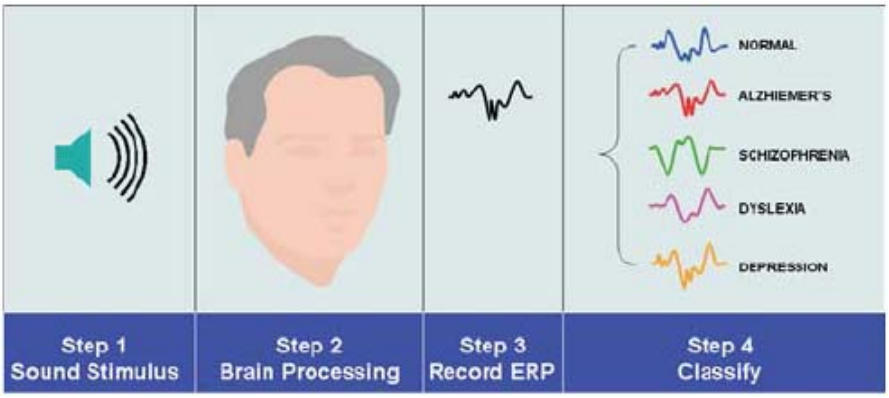


Figure 20: Diagnosis of neurological disorders by ERP 'brain waves' (by courtesy of Neuronetrix).

[29] http://www.spectrum.ieee.org/sep06/4427
[30] cf. http://www.eurekalert.org/pub_releases/2007-02/m-rsi020607.php
[31] cf. www.neuronetrix.com

In this field of signal processing, insights from brain research inspire cognitive scientists, and vice versa (see textbox). For example, the so-called *neural networks* in computer science express a concept borrowed from the cognitive area.

'I certainly see convergence between information science and cognitive neuroscience. Especially the artificial neural networks devised by information scientists are very inspiring for brain researchers. The artificial neural networks help one to view the brain functions differently. The classical thinking in brain research has been much in terms of mapping brain functions in words like attention, working memory, perceptual organization, long term memory, short term memory. The artificial neural networks show that seemingly complex work can be done by simple local operators. Currently we collaborate with the research group of prof. Arnold Smeulders of the Mathematics and Information Science faculty of the University of Amsterdam. These researchers analyse images by means of computer algorithms. For us as visual researchers their approach is both interesting and confronting. Their image analysis methods work intuitively and naively and start with simple contrast distributions, quite a bit like the human visual system. These seemingly simple approaches generate practical results. Some analyses discern whether a picture has been taken inside or outside, others whether there are people in the scene or not. An analysis of the light distribution can tell whether a picture is taken at home or at the office. These simple parameters show quasi cognitive hints that help steer more detailed image analysis. It is impressive and also very different from classical image processing approaches. Originally the image processing algorithms tried to interpret scenes in terms of cognitive concepts. They would try to figure out which elements or objects were detectable in a scene and would use these pieces of evidence to interpret the kind of scene. The current image analysis algorithms work the other way around. They are based on global parameters. For example they tell whether a scene is such that chairs could be expected. During further processing the actual chairs in the scene can then be actively searched for. The visual perception of humans and animals works quite like that. As scientists see it now, first a global scene is built up, and this is later filled in more detail.'

Interview with prof.dr. Victor Lamme (Universiteit van Amsterdam)

6.1.3 Convergence between biotechnology and ICT

The convergence of biotechnology and ICT resembles the convergence of cognitive sciences and ICT. As with cognitive systems, biological systems may inspire the ICT field. Examples are camera surveillance systems that imitate the human eye[32]. As in cognition, the storage and processing of biological data requires ICT. An example is the integration of biosensors in a smart ICT environment. The so-called fields of *Bioinformatics* and *computational biology* involve the use of techniques including applied mathematics, informatics, statistics, computer science, artificial intelligence, chemistry, and biochemistry to solve biological problems usually on the molecular level.

6.1.4 Convergence between cognitive- and nanotechnologies

The convergence of cognitive- and nanotechnology resembles the convergence of bio- and nanotechnology in the sense that developments in nanotechnology are applied to

[32] http://pass.telin.nl/

cognition (cognitive systems can be measured or manipulated at the 'nano level'). Often more than the two technologies (i.e. cognition and nanotechnology) only may be involved. A nice example is the potential use of nanotechnology probes for Deep Brain Stimulation (see Figure 17 in Section 5.2 for an explanantion of Deep Brain Stimulation). Instead of using 'traditional' electrodes, the possibility of using conducting nanostructured polymeric wires is now being explored, as shown in Figure 21 (Llinás *et al.*, 2005).

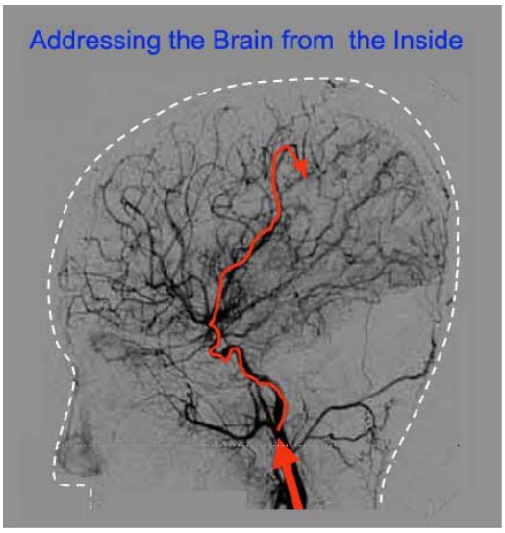


Figure 21: Using nanotechnology probes to address the brain from inside (by courtesy of Mihail Roco (2007b))[33].

6.1.5 Convergence between nanotechnology and ICT

In many ways nanotechnology and ICT developments are stair-stepping on one another. On the one hand nanotechnology and nanoscience enable further miniaturisation and the development and use of new materials in (opto-)electronic components for ICT equipment. On the other hand, no 3D model of nano material structure, or catalytic production of nano material or high precision lithography planning for nanofabrication can exist without a supporting high-speed computation.

In electronics the very progress of semiconductors lies in the domain of nanotechnology. Understanding and predicting the structural properties and homogeneity at the nanometre level requires the latest insight from nano-science. Likewise, production methods for nano materials and integrated electronic circuitry are converging. New production methods from nanotechnology are expected to be adopted by the electronics industry, such as creating and growing functional polymers, doped crystals or alloys, and newly discovered materials like nanotubes and graphene (Geim and Novoselov, 2007).

Convergence is highest where the statistical classical paradigms of magnetic, electromagnetic, and/or electronic properties give way to particle or quantum properties, such as in spintronics, quantum computing, single electron switching, and optical switching. Eventually such technologies could enable femto-second computations and likewise terahertz clock frequencies. Communication throughputs can grow further, while memories based on these technologies can store large quantities of data with little power consumption.

[33] See also: http://www.nsf.gov/crssprgm/nano/reports/nni_roco@picmet.pdf.

All optical switches applying bi-stable properties of nanoscale crystals, hard disk memories applying the giant magneto-resistive effect, and non-volatile MRAM memories applying the giant tunnel magneto resistive effect are early examples of such technology convergences. A more recent success is reported by scientists at IBM TJ Watson Research Center who combined carbon nano tubes with a silicon substrate to obtain a 'nano-chip'.[34] Nanoscale quantum mechanical memory elements operating at room temperature have been demonstrated by scientists at Harvard, who were able to measure the nuclear spins of individual C-13 atoms in a diamond lattice[35].

Moore's Law is the empirical observation that the number of transistors on an integrated circuit for minimum component cost doubles every 24 months. However, once continuing miniaturization will end. New fundamental developments in nanophysics may enable new applications 'beyond Moore.' The current research on new concepts for molecular-scale devices and integrated circuits tackles this area.

'Yet the nanotechnology is very promising. Toshiba develops new batteries using nanotechnology to increase the surface area where the relevant chemical reaction to free electrons takes place. That is a good example of a nanotechnology application. Nanotechnology enables one to downscale details. But this will not mean an outrageous improvement in battery technology. A factor 2 would get people really excited whereas such improvements happen in chip technology every 18 months.'

Interview with prof.dr. John Long (TU Delft)

6.1.6 Convergence between biotechnology and cognitive sciences

Developments on the convergence of biotechnology and cognitive sciences have always been under public scrutiny. Depending on 'zeitgeist' fields like biological psychiatry, neurosurgery, genetics, and to a lesser degree neuroscience, psychopharmacology, and physiology and biochemistry have met public resistance. Most notorious in this respect is the Buikhuisen case in the late 1970s in the Netherlands where a popular columnist raised a public and even academic protest against scientific research into the biological basis of criminal behaviour. The central issues here are whether the human (or animal) mind has a neurological and chemical basis, and whether mental illnesses exist at all, and whether it would be ethical to treat mentally ill people against their will.

Much progress has been made in understanding the biological basis of cognition, and likewise the systemic coherence of brain-areas the influence of neuro transmitters, and the neurological pathways that exist in the brain and body, and possible ways to stimulate or block these connections by ways of medication, surgery, electro-stimulation or 'classical' counselling.

The understanding 'how the mind works' has likewise boosted the approach and methods in non-invasive cognitive neuroscience. A better understanding leads to new and testable hypotheses. Especially the advent of fMRI enabled cognitive scientists and psychiatric researchers alike to conduct experiments where subjects' brains were observed as they functioned. The resolution of fMRI lies in the mm range. In terms of neurological functioning, this is still coarse grained. Therefore, electrophysiological experiments both

[34] http://www.cio.com/article/19472/IBM_Shrinks_Circuit_With_Nanotube
[35] http://www.sciencedaily.com/releases/2007/05/070531142118.htm

in animals, men, and in vitro will teach more about the exact working of specific brain cells, areas, and pathways.

'Among psychologists there has long been a growing understanding that the idea of free will is a post hoc construct. The stream of consciousness makes a story out of what is experienced after the fact. Findings in consciousness research have only further decreased the supposed influence of thoughts on behaviour. Some people say that free will does not exist and that people should therefore not be held accountable for their behaviour, but I do not agree. The conscious thought about free will may not exist, but that does not mean that people are not responsible for what they do.'

Interview with prof.dr. ***Victor Lamme*** *(Universiteit van Amsterdam)*

6.2 Expected future convergence points

In this section we focus on some more fundamental principles that would allow an 'evolutionary convergence.'

Convergence with nanotechnology

In order for the biotechnology, ICT, and cognitive sciences (BIC technologies) to benefit from nanotechnology, they should meet the following requirements:

- Possibility: either of the following should hold:

  1 It should be possible to use nano-tools for discerning, isolating, manipulating, or implementing B, I, or C systems of sufficiently small sizes (to exploit the benefits of nanoscale), but sufficiently high functional or behavioural complexity (to exploit the specific benefits of the B, I, or C technologies).

  2 It should be possible to build nanoscale systems that mimic or enhance particular behaviours or functions of B, I, or C sub-systems.

- Necessity: nanotechnology should complement the functional properties of B, I, or C systems. The new functions implemented on nanoscale structures should not be possible or practical to be achieved through any combination of B, I, or C systems.

Convergence with biotechnology

The convergence of nanotechnology, ICT, and cognitive sciences (NIC technologies) with biotechnology will happen when either of the following holds:

- NIC systems can exchange energy with biological structures in a predictable, measurable, or controllable way.

- Biological models (structural or functional) can explain the functioning of NIC systems.

- Biological functions can be replicated in NIC structures.

Convergence with ICT

The key requirements for a full convergence of information and computer technologies with any of the other technologies are:

– Discerning and inducing quantifiable (especially binary) stable states of a nano-, bio-, or cognitive (sub-) system.

– Controlling deterministically the transitions of these states.

– Applying the controls to well-defined subsystems of minimal complexity.

The first requirement pertains to the ability of 'reading' and 'writing' arbitrary values from or to the target subsystem. The requirement does not necessarily mean that the target subsystem should remain forever in that state, but rather that a change of state will always be the result of an internal or external action, and that the action and its results are explicit (i.e. produce an observable effect). An example is the rotaxane molecule (see section 2.2 / footnote 10) that can exist in two configurations, which in turn can be interpreted as the two binary states of a switch, or memory element.

The second requirement makes explicit the distinction between the macroscopic properties of a complex system, which may result statistically, and the state of the system as a linear superposition of the known states of each individual subsystem.

The third requirement ensures the ability to control independently small parts of the target system, such that complex state transitions (behaviours) can be implemented.

Convergence with cognitive sciences

A full convergence of nano-, bio-, and information (NBI) technologies with cognitive sciences will be possible when the following two requirements are met:

– Cognitive functions are identified and explained in terms of abstract functional models that can be implemented on NBI structures.

– NBI systems can act upon cognitive systems in a way that predictably influences the state of the cognitive system. Moreover, the cognitive system has to experience these induced states as meaningful and coherent.

6.3 Natural convergence paths: a model for convergence

A further analysis of the above requirements leads to the following observations:

1 Nanotechnology and biotechnology deal with *structures* that have different underlying nature, but evolve toward comparable architectural complexity.

2 Cognitive sciences and ICT deal with *functionalities* implemented on structures of different nature, but evolve toward comparable algorithmic complexity.

Therefore two types of convergence can be identified: structural and functional. The main effect of these convergence processes is the achievement of reciprocal

compatibility between the converging technologies. This reciprocal compatibility could be regarded as a sine qua non condition for the paradigm shift discussed earlier.

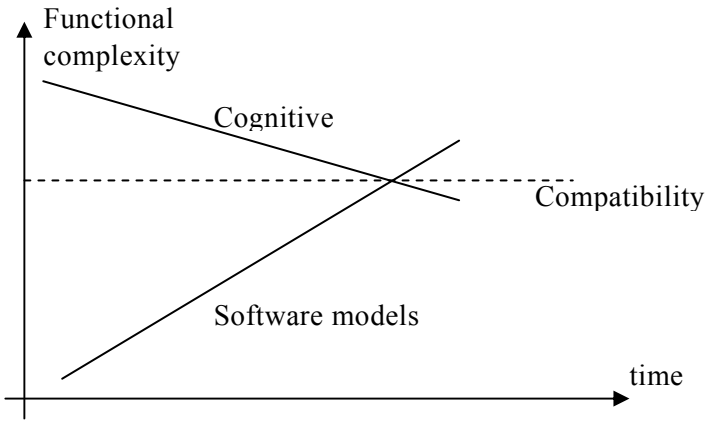


Figure 22: Convergence along a functional dimension.

Natural convergence paths are easily identifiable between cognitive sciences and ICT at functional level (see Figure 22). On the one hand the cognitive models tend to isolate and explain cognitive functions of lower complexity, which admit comprehensive computational descriptions. On the other hand, data processing and analysis techniques become increasingly complex. At some point, the complexity of cognitive functions will become manageable for the future ICT solutions.

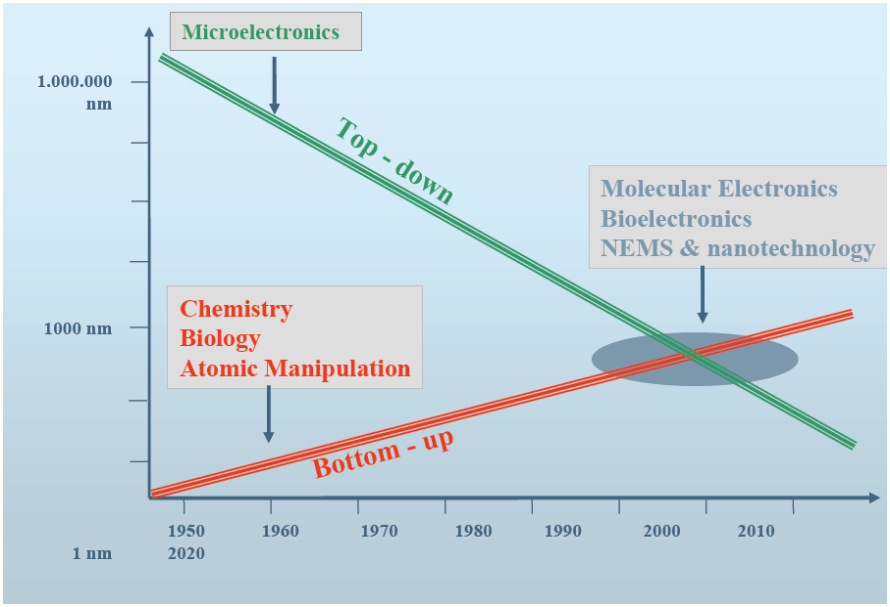


Figure 23: Convergence along a structural dimension (by courtesy of IMEC[36]).

At structural level, the most obvious convergence can be identified between bio- and nanotechnologies, where top-down and bottom-up approaches come together (see Figure 23).

[36] http://www.imec.be/

Another set of convergence paths is predictable between structures and functions. ICT solutions (complex software) are easily applicable to artificial nanostructures. The achievable functional complexity, however, depends on the architectural complexity of the nanostructure.

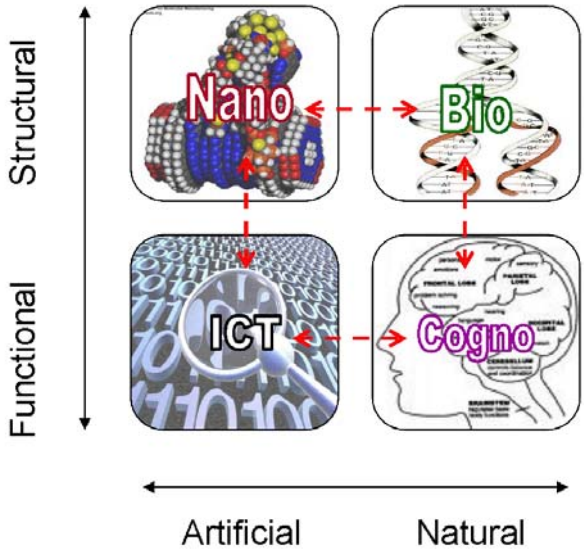


Figure 24: A model for natural convergence along two dimensions.

By generalising these remarks we can conjecture that convergence will occur in a first instance between nanotechnology and ICT, nano- and biotechnologies, biotechnology and cognitive sciences, and cognitive sciences and ICT, as suggested in Figure 24.

6.4 Disruptive technology developments

Except for evolutionary developments, convergence may also lead to disruptive developments in application areas. Paradigm shifts due to convergence, however, are difficult to predict. History shows that short-term expectations are often over exaggerated. As soon as the first successes are shown, everything seems possible. Practice often behaves in a wilful manner, however. That is what we observe in, e.g., 'brain reading' and 'face recognition'. But, long-term expectations are often underestimated because of changing lines of thought: paradigm shifts which can not be imagined in advance and therefore are difficult to predict (see also Table 5). Due to our 'conceptual limitations,' it is easy to predict 'first order' effects, almost impossible to predict higher order effects. The only thing we can say is that (disruptive) convergence shows up in applications. We will try to sketch some application scenarios containing higher order effects ('new application paradigms') in Chapter 8.

Table 5: Failed predictions of experts of their time[37].

'It's a great invention but who would want to use it anyway?' -- Rutherford B. Hayes, U.S. President, after a demonstration of Alexander Bell's telephone, 1876.

'Radio has no future.' -- Lord Kelvin, Scottish mathematician and physicist, former president of the Royal Society, 1897.

'Airplanes are interesting toys but of no military value.' -- Marechal Ferdinand Foch, Professor of Strategy, Ecole Superieure de Guerre, 1904.

'That the automobile has practically reached the limit of its development is suggested by the fact that during the past year no improvements of a radical nature have been introduced.' -- Scientific American, Jan. 2 edition, 1909.

'There is not the slightest indication that nuclear energy will ever be obtainable. It would mean that the atom would have to be shattered at will.' -- Albert Einstein, 1932.

Transmission of documents via telephone wires is possible in principle, but the apparatus required is so expensive that it will never become a practical proposition.' -- Dennis Gabor, British physicist and author of Inventing the Future, 1962.

'By 1985, machines will be capable of doing any work Man can do.' -- Herbert A. Simon, of Carnegie Mellon University - considered to be a founder of the field of artificial intelligence - speaking in 1965.

'There is no reason anyone would want a computer in their home.' -- Ken Olson, president, chairman and founder of Digital Equipment Corp. (DEC), arguing against the PC in 1977.

6.5 Conclusions

The fields of nano, bio, information and cognitive technology are each multidisciplinary areas, combining several disciplines. Still, they may further integrate as generally meant by *converging technologies*. Converging means how nanotechnology enables biotechnology to develop new sensors as well as contributes to the miniaturization of information technology sensors to support monitoring applications. Converging means that biotechnology enables nanotechnology by providing mechanisms of cellular recognition for forensic research. Converging also means that information technology provides the processing power or visualization tools to enable the use of nano-bio sensors for risk analysis and assessment.

In that sense, strictly speaking a DNA database is an integration (rather than convergence) of bio and ICT technology, monitoring through RFID tags is not even an integration but only ICT technology, and a lab-on-a-chip application is not even nanotechnology but micro technology. However, paradigm shifts due to convergence are difficult to predict. Since integration may be a first step to further convergence, we merely investigated natural ('evolutionary') convergence paths. Two types of convergence can be identified: structural and functional.

[37] http://en.wikipedia.org/wiki/Failed_predictions

1 Nanotechnology and biotechnology deal with *structures* that have different underlying nature, but evolve toward comparable architectural complexity.
2 Cognitive sciences and ICT deal with *functionalities* implemented on structures of different nature, but evolve toward comparable algorithmic complexity.

The main effect of these convergence processes is the achievement of reciprocal compatibility between the converging technologies.

7 Relevance of Converging Technologies for security applications

The previous chapters have focused on NBIC technologies and their development. From these chapters we gain an insight into the dependability of all kind of expectations with respect to the futuristic application of technology developments. Knowing what is realistic, we focus on the application of these technologies in the domain of the Ministries of Justice and Internal Affairs in this chapter. How can the authorities use the converging technologies? Or, how may others use them and herewith have an impact on the policy or activities of the government? The previous chapters are –as far as possible– independent of any application domain. This chapter shows which technologies are relevant for the domain of the Ministries of Justice and Internal Affairs.

During the 'mapping' of technology onto the application domain, the technology is leading. So this chapter is 'technology push'. A problem-driven approach starts with application requirements whereupon technological solutions are searched. We start with the (more or less autonomous) technology developments and search for usability in an application domain. However, because of the broadness of the applications field, we focus the discussion of technology applicability around three cases:

- Case 1: Monitoring and following objects or persons and remote intervention in case of undesired movements and relocations (in short: *Monitoring and immediate action*);
- Case 2: Improving and developing forensic trace analysis (in short: *Forensic research*)
- Case 3: Profiling, identifying and observing persons with an assumed security risk (in short: *Profiling and identification*).

While investigating the meaning of technology developments for these cases, we focus on possible applications, not on desired applications. That is, we do not take legislative, ethical or social considerations into account. These impacts will be analysed in Chapter 9. In this chapter, we focus on possibilities. However, we do not write science fiction but focus on the likely applications for the next 15 years. Therefore, current developments in the application domain are taken into account and may be extrapolated towards the future. We survey the application of technology for the three cases in the next 5, 10 or 15 years.

7.1 Case 1: Monitoring and immediate action

7.1.1 Characterising the case

The case 'Monitoring and Immediate Action' basically refers to tracking and tracing objects or persons, and being able to somehow intervene if necessary. An immediate reason to select this case has been the current (experimental) use of RFID tags to monitor prisoners (Kruissink *et al.*, 2007)[38]. In general, positioning and/or communication technologies like GPS or RFID tags in combination with a return channel (such as UMTS) can be used to track and trace objects or persons. How do these developments

[38] Also, see: http://www.geodan.nl/nl/markten/veiligheid/detentie-concept-lelystad/

extrapolate into the future? Cars already get GPS systems to trace them in case of theft. It is possible to remotely bring a car to a halt[39].

As mentioned before, the tagging of persons currently happens in experiments with prisoners. A next step may be the use of a biochip (instead of using an arm- or foot-badge). The question arises whether these developments continue with the use of still more accurate sensors or (brain) implants, or whether some devices can also be used to intervene, either autonomously or remote-controlled. From an application point of view still other questions arise. A main goal of the prison is to reduce recidivism. By using monitoring technology, therapists can also get a better picture of the individual prisoner. In this way they may predict or anticipate on behaviour. This may help improving the individual treatment and herewith reduce recidivism. Using tracking and tracing technology to extend concepts like being under house arrest may even enable applications like a 'prison-without-walls'.

Besides monitoring people to prevent them from doing wrong, one may also monitor persons to protect them. For example, to protect (young female) applicants for asylum who sometimes disappear and end up in prostitution. So technology may be used both preventatively and repressively. Also, additional technologies may be used to monitor persons in virtual environments (behaviour on Internet).

7.1.2 Application trends

Monitoring is closely related to acquiring location or behaviour information, relating this information to identities (persons), and sharing this information. Clearly privacy issues arise. Therefore, we asked our web panel their opinion on the following statements (see Appendix B.3.1):

– Persons have more and more identities, both in real life and in the virtual world.

– People will trade privacy for increased (perceived) social security.

– People will share their location information with the authorities.

The panel could give the answer in a range from disagree to agree in five steps. The question whether people will trade privacy for security shows the clearest response. The result is an almost linear increasing graphic art from disagree to agree. So the general belief is that people are willing to sacrifice privacy for social security. However, that does not necessarily mean that privacy becomes less important. Remarkably, the question about revealing your location information gives a perfect symmetric, almost normally distributed result over the entire disagrees-agrees range. Does this mean the 'average person' is more or less indifferent to this issue? To quote a respondent: 'I'm not sure that this is what people want, but it is what they do already. Mobile phone data give a pretty good clue now and this will become better.' We interpret the both questions together as *privacy is important, but people are willing to trade it for security*.

With respect to the question of people having more and more identities, the meanings are diverse. Again, the average is rather neutral (though slightly deviating to agreement) but

[39] See e.g. http://www.carpages.co.uk/news/stop-car-crime-by-text-22-02-05.asp

most respondents either disagree or agree. This might be caused by different interpretations of what an identity is, but we can not draw a clear conclusion from this.

7.1.3 Relevant technologies for monitoring and immediate action

Currently, mainly ICT technology seems to be used for monitoring and (remote) immediate action. Examples are:

- Using video surveillance and related image analysis tools for pattern recognition or face recognition (see also the profiling and identification case in section 7.3).
- RFID chips are used to tag prisoners and track or trace them within a prison. This is mainly an indoor activity.
- The RFID chip (arm bracelet) is also used for identification in case of using several services provided via a computer screen. In principle, this allows individual monitoring of using these services.
- GSM technology (or other communication technology, like WiFi or Bluetooth) can be used track and trace mobile phones and herewith their owners. This can be done 'live' on a wide-area (outdoor) level.
- Position technology, in particular GPS can be used for the same purposes. Note that the future European version of GPS –called Galileo– allows two-way communication (required for remote action) as well.
- Mechanical technology like a 'knee-lock' can be used to prevent persons from running away. Using available communication technology, these locks can be remotely controlled.

From our literature study, as well as from expert opinions (see Appendix B), we expect the (future) technological developments as shown in Figure 25 to be relevant for monitoring and immediate action. The figure lists the abovementioned ICT developments, in which it adds aspects of real-time processing (for monitoring geographic areas) and cooperation between several (autonomous) systems. This results in the items of tracking objects using several cameras (handover), the integration of data from several sources, and interoperability between (heterogeneous) systems. The use of cognitive models may improve the performance of information systems (artificial perception). From the bio and cognitive fields, sensor technology is relevant, i.e., sensors in (implants) and on the body or brains. Also, these technologies enable actuators for immediate action (electro-stimulation, interaction with cells). These actuators might be based on nanotechnology.

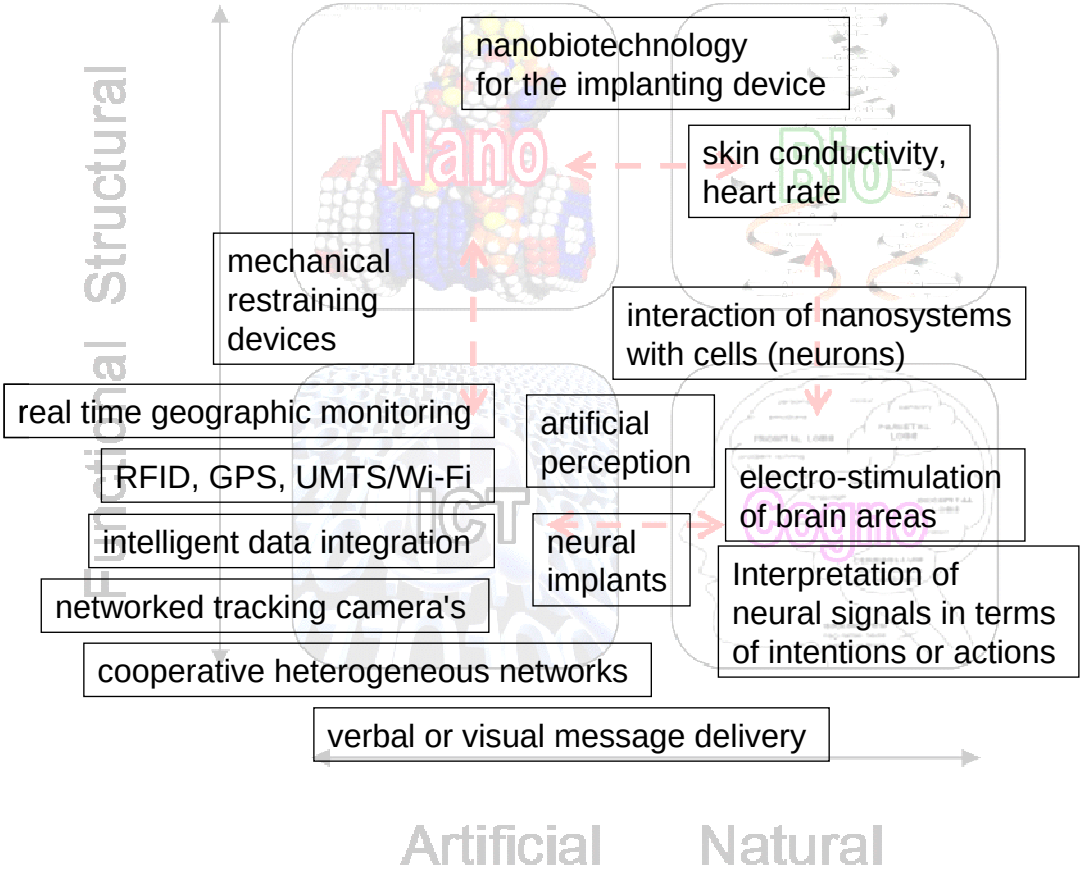


Figure 25: Main relevant technologies for monitoring and immediate action.

From the discussion in our workshop (Appendix A.5), we conclude the following possibilities. First of all, we have the *on-line registration of variables*. As indicated before, at the moment mainly ICT technologies are being used for monitoring purposes, like location technologies. However, all kind of medical variables could be sensed and transmitted. Sensors can be in the body, like biochips. For example, during the 4-day walking event in Nijmegen in 2007, persons swallowed a sensor to measure their temperature on-line while walking[40]. Examples of sensors on the body are those that detect sweat (or rather skin conductivity) as an indicator of e.g. fear. Biosensors may be based upon different nanotechnologies. Examples of sensors to obtain information pertaining to cognitive processes are the fMRI and EEG scans. Though fMRI is not particularly a 'wearable' sensor, EEG could be. Due to ICT technology, people will always be on-line. The overall result is that more and more indicators (variables to be measured on-line) become available. Improving human-computer interfaces strengthen this trend. Also, besides internal indicators (with respect to the body), environment indicators are available. Positioning has already been mentioned as an example.

A second issue is *risk assessment*. From all the available indicators, conclusions have to be drawn, e.g., with respect to the threats that the monitored person is facing from external factors, or posing to other people. The combination of bio-, cognitive- and ICT

[40] http://www.nijmegenonline.nl/nieuws/vierdaagsepil-tot-273%C2%BAc-geen-oververhitting/

indicators may be used to assess these risks. Similar risk assessment may be done by aggregating sensor information from multiple persons for other types of security problems, e.g. crowd monitoring. On this point, the monitoring and immediate action case (case 1) is not essentially different from the profiling and identification case (case 3). As a third case, persons seeking asylum can be monitored, assessing the risk that something happens to them (e.g. using fear as indicator). The logging of sensor information individually or collectively over large periods of time can be used in combination with data mining and pattern discovery techniques for ever better ways to predict what is going on or going to happen next. For example, one day one may distinguish whether someone 'disappeared' voluntarily from when this was done by force.

As indicated in the technology overview, the value of 'brain reading' is often over exaggerated. However, whereas it may be difficult to draw conclusions on a higher semantic level from EEG signals or other brain activity sensors only, the combination with signals from other biosensors, location, and sensed environment data may enable to learn different associations between cognitive processes, sensor data, and external events. These associations, combined with experts' analysis could become a useful tool in predicting some criminal acts.

The third point is *restraining* persons in well-defined cases, or more general the immediate (remote-controlled or autonomous) action. Currently, restraining can be implemented using a knee-lock, which may limit the walking speed (passive). This restraining may become more intelligent, like an engine being switched off in case the driving persons falls asleep, etc. Also, micro- or nano-devices might allow active restraining. Note that pharmacological restraining is also an existing possibility.

Fourth we have to deal with the issue of *tampering*. As soon as technology is used, people may try to tamper with the technology. As soon as tampering is discovered, actions may be taken ('restraining'). Also, sensors within the body are more difficult to tamper with.

7.1.4 Expectations for the next 15 years

What about the timeline of the technology forecasts of the previous section? We posed our expert panel on Internet the following question (see Appendix B.3.1): 'How long will it take before the following innovations become reality?'

- Tagging prisoners detained at her Majesty's pleasure (the Dutch 'TBS') with implanted RFID tags.

- Positioning technology combined with bio- and nano sensors enable tracking and tracing individuals.

- Movement of cars or persons ('knee-lock') can be blocked either manually from a distance or automatically based on sensor information (like entering a virtual trespassing border).

- Electronically controlled animals can be sent out for surveillance (or for attack).

- Converging technologies make it possible to forecast who will become recidivist and who will not.

– Converging technologies make it possible to influence the perceived recollection of persons (to be used therapeutically).

– Influencing behaviour by brain implants.

– Prison without walls, i.e., a virtual imprisonment enforced by technology.

– Selective chemical or biological substances only affect people with certain genetic traits.

The possible answers are within 5 years, within 10 years, within 15 years, more than 15 years, and no opinion. Figure 26 shows the answers of the experts who felt themselves confident to answer this question.

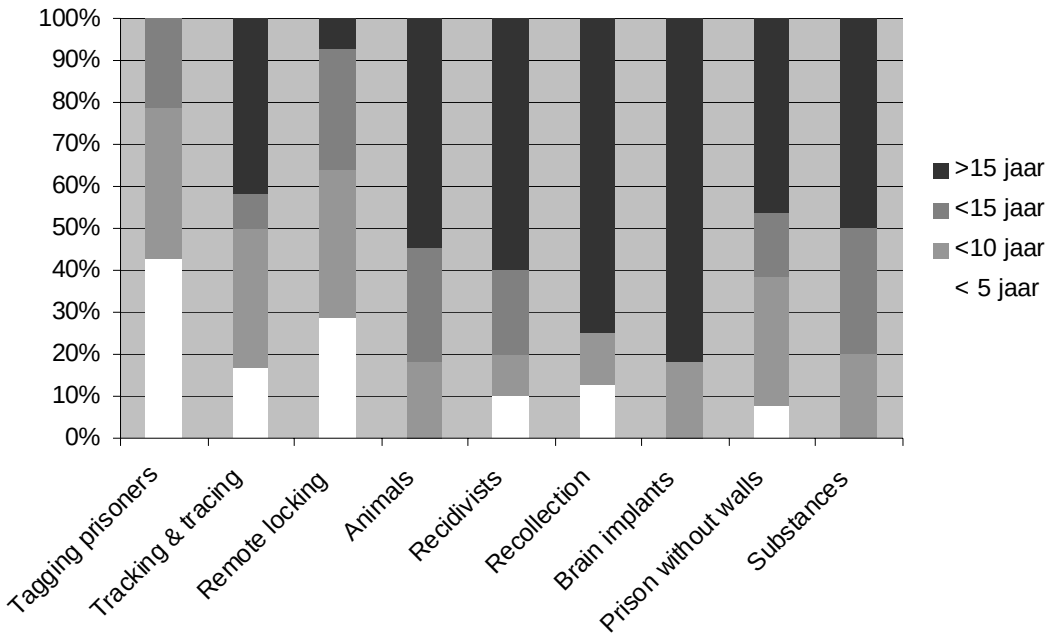


Figure 26: Expected applicability of technology for monitoring and immediate action.

We observe that tagging prisoners or persons being detained during her Majesty's pleasure (the Dutch 'TBS') with an implanted RFID chips ('biochip') and blocking cars or persons automatically based on sensor information are expected on the shortest terms. A striking issue is that the majority of respondents expects that it still takes 10 years (or more) to get these technologies to be applied in monitoring respectively immediate action, whereas we are talking about technologies that are in principle available today! Apparently, difficulties in bringing this technology to practice are expected.

Tracking and tracing individuals is expected on a bit longer term. Also, the opinions are diverse (50% within 10 years, 50% more than 10 years). This technology is available today. However, the powering requirements of these devices make it impossible to have these devices implantable[41].

[41] Unless body movements, like heart vibrations, can be used to generate power? See also the example mentioned in http://news.bbc.co.uk/2/hi/technology/6272752.stm .

New concepts like a prison without walls (extrapolations of the house arrest) and the use of selective chemical or biological substances to affect people with genetic traits are expected over at least 15 years.

Not expected for the coming 15 years as well are electronically controlled animals that can be sent out for surveillance (or for attack). Similarly anticipating on criminal behaviour or recidivism, influencing memories of persons (to be used therapeutically) and influencing behaviour using brain implants, are also not regarded as feasible within 15 years. Coincidentally or not, all these applications are closely related to cognitive sciences.

7.1.5 Conclusions for monitoring and immediate action

Based on our literature study, interviews, web survey and workshop discussions, we suggest that the following applications in monitoring and immediate action will be technically feasible by 2022:

- Individually worn sensors, in particular tagging prisoners or persons being detained during her majesty's pleasure (the Dutch 'TBS') with an implanted RFID chip (short term).

- Wearable personal monitoring devices with data recording and on-line communications capability (short term).

- Tracking and tracing individuals in civic areas.

- Implants (or prostheses) that mimic or even augment human biological functions, but no selective memory erasure and no behaviour manipulation by brain implants.

- Blocking cars automatically based on sensor information (short term).

- Objects (e.g. clothes) that respond to external stimuli (like location, heart beat).

- Wireless Internet available worldwide (short term).

7.2 Case 2: Forensic research

7.2.1 Characterising the case

Forensic research is the process of finding traces, analyse them, and eventually turn them into legal evidence. New technologies make it possible to establish new kinds of proof positive. An example is using DNA material for identification, which is only possible thanks to recent technology. What kind of new proof positives does NBIC technology make possible?

New technologies may even be required because of the necessity to analyze minute traces (level of molecules). Also, where e.g. a fragment of glass could formerly be uniquely identified due to its imperfect production, the current glass production requires more refined analysis techniques for distinguishing them. If nanotechnology makes the surface of objects 'free of any trace', clearly the forensic research has to find a solution.

Current NBIC technologies do not only make the current forensic research process more effective or more efficient, it may completely change the way of working. For example, an analysis that used to take several weeks or months at the laboratory may currently be done rapidly at the place of offence thanks to e.g. lab-on-a-chip technology. This means that analysis results may steer the search for traces, in this way mixing phases that always have been sequentially separated before.

The miniaturising and commodification also means that techniques that used to be available to the large institutions only, become available to individuals, who can do the same analyses. This may cause drastic social and institutional effects.

7.2.2 Application trends

Given the case characteristics, we asked our web panel their opinion on the following statements (see Appendix B.3.2):

– Traces are becoming smaller and smaller - a single cell may be enough for analysis.

– Technology which used to be available in specialised labs (like the Dutch NFI) will become available to everyone - with tools becoming smaller in size.

– Materials become more perfect and herewith less distinguishable.

– DNA databases will be internationally coupled.

– Criminality shifts towards the virtual world as well.

The panel could give the answer in a range from disagree to agree in five steps. The experts agree that traces are becoming smaller, DNA databases will be coupled internationally, and criminality shifts towards the virtual world as well. Half of the experts agree that lab technology will become available to everyone, the other half disagree or judge neutral. Apparently the opinions diverge on currently specialised tools becoming available to the public, which indirectly refers to the organisation of forensic research. Finally, the experts find it difficult to judge if materials will become more perfect and less distinguishable.

7.2.3 Relevant technologies for forensic research

From our literature study, as well as from expert opinions (see Appendix B), we expect the (future) technologies developments as shown in Figure 27 to be relevant for forensic research. Nanotechnology is expected to be important for this case. Nanotechnology enables means to find small traces (sprayers) or to analyse traces (lab-on-a-chip). Information technology can be used for both processing the large amounts of information (pattern recognition, quantum computing) as well as for collecting information (e.g. social software to involve citizens). Finally, DNA is important in forensic research.

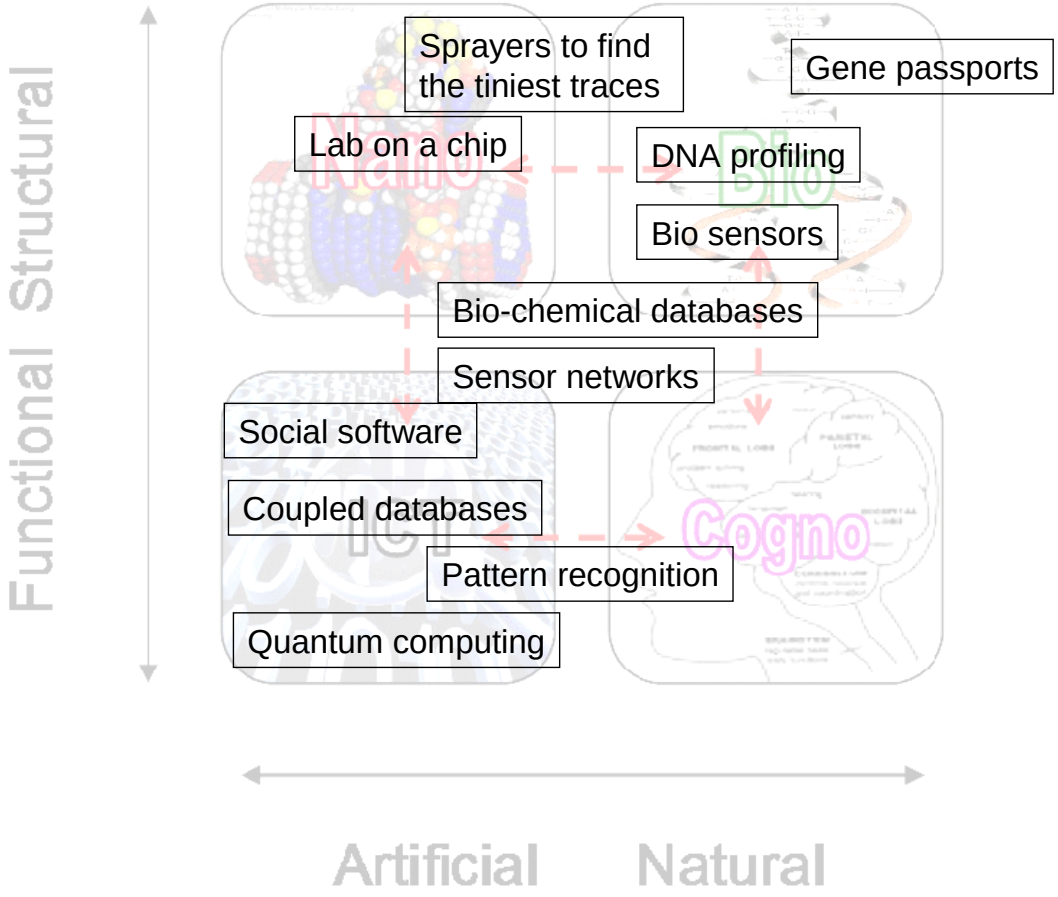


Figure 27: Main relevant technologies for forensic research.

Genetic databanks are a big trend, which can be observed everywhere in research centres around the world. These genetic databanks will typically not contain complete genome sequences but rather a characterisation of genomes of individuals and groups at the level that matters to healthcare and public security.

Lab-on-a-chip allows the performance of complex analyses of viruses, chemical or biological compounds, by non-specialists, or in the absence of laboratory equipment. A DNA chip increases the analysis speed of biomarkers by performing tens of thousands of analyses at a time.

Genetic analysis is likely to improve both with regard to accuracy, speed, and ease of operation. Bio-informatics will in many respects determine the speed of analyses. Technical advances in genomics and population genetics will stimulate a further development of this discipline. Fast and massive whole genome sequencing technologies will enable reliable DNA analyses of even the most complicated mixed DNA samples. Optical sensing devices allow for the imaging and diagnostics of nano-particles. Finally the introduction of SNP typing technologies[42] will facilitate the dry analysis of DNA.

[42] Single nucleotide polymorphisms (SNPs) are DNA sequence variations that occur when a single nucleotide (A,T,C,or G) in the genome sequence is changed, which occur approximately once every 100 to 300 bases.

The link between bio- and information technology is important for the processing and analysis of data. Advances in quantum computing may be relevant for the processing of the vast amounts of data (a single human genome is already 6 Gigabit of data) because quantum computing power is supposed to scale in an exponential way with the number of processors (whereas current computers scale in a linear way). As for the algorithms, pattern recognition techniques will be important to make sense of this data.

Finally, another important technology for forensic research is 'web 2.0' or 'social software' which facilitates the working together of people via the Internet. This technology might be used to quickly involve experts in analyses.

7.2.4 Expectations for the next 15 years

With respect to future forecasts, we posed our expert panel on Internet the following question (see Appendix B.3.2): 'How long will it take before the following innovations become reality?'

- Biotechnology provides mechanisms of cellular recognition for forensic research.
- Nanotechnology-based sprayers can be used to sprinkle a room and find the tiniest traces.
- Nanotechnology enables the production or treatment of objects (like clothes, cars, et cetera) so that hardly any trace can still be found.
- Portable DNA profiling devices.

The possible answers are within 5 years, within 10 years, within 15 years, more than 15 years, and no opinion. Figure 28 shows the answers of the experts who felt themselves confident to answer this question.

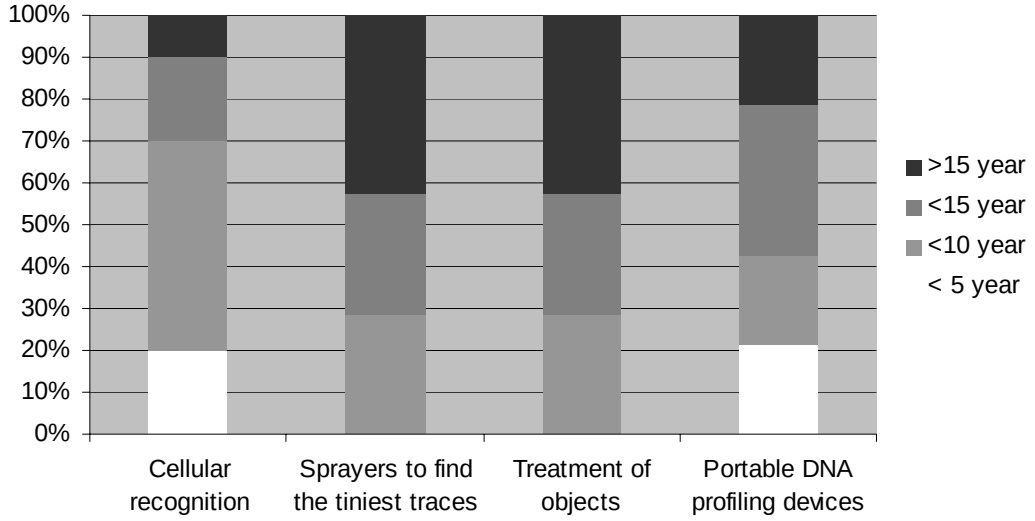


Figure 28: Expected applicability of technology for forensic research.

Most experts agree that cellular recognition will be feasible within 10 years. Sprayers to find tiny traces and smart materials (e.g. clothes, cars etc.) which barely leave any traces

are expected on the long term (15 years or more). Portable DNA profiling devices are expected on the mid-long term (10 to 15 years).

In the expert workshop the following technologies were considered feasible to be applied within 15 years (see also Appendix A.5):

- Portable laboratory/ analysis instruments (DNA, chemicals)
- Large scale biochemical databases
- Single molecule detection
- Biomarker palettes for behaviour
- Multiple parameter determination
- Fast processing of information
- Coupled information systems with pattern recognition
- 3D image of crime scene, real time contact with experts
- Fast DNA profiling in small portable analysis instruments, which are able to combine DNA information with biological information
- Information derived from proteomics, metabolites and trace elements
- Sensors which are able to provide an integral and reliable air analysis
- Deriving information from biological stains:
    - Cellular origin of biological sample
    - Geographic origin of donor
    - Visible characteristics of stain donor (e.g. skin, eye colour, age)
    - Age of stain
    - Psychological status of a person at the time of crime
- Integration of micro sensors with macro sensors (from microscope to satellite)

7.2.5 Conclusions for forensic research

Based on our literature study, interviews, web survey and workshop discussions, we suggest that the following applications in forensic research will be technically feasible by 2022:

- Rapid forensic evaluations from very small amounts of materials (short term).

- The use of new families of (miniaturized) highly selective, accurate and sensitive biological sensors.

- Computational devices –like ‘lab-on-a-chip’– becoming commercially available.

- Objects (e.g. clothes) that respond to external stimuli like the availability of specific (biological) substances.

- Powerful wearable computers / laboratories (short term).

- 3D visualisation of crime scenes.

- Resistant textiles, leaving hardly any traces (long term).

7.3 Case 3: Profiling and identification

7.3.1 Characterising the case

To search for persons with an assumed risk for society, profiling can be used. In this sense, profiling means describing the characteristics of a criminal or terrorist (for example in terms of behaviour patterns), and use this profile to identify persons with similar traits in the immense crowd at, e.g., an airport or railway station. Of course, profiling and identification is not only a matter of physical observation or video surveillance. The risk analysis will be based on available information from whatever 'intelligence' applications. Then, profiling also becomes the prediction of (or anticipation on) expected behaviour based on all available information.

Identification is also the term that is generally used for looking for a specific person – whose identity is known– in a crowd. So we typically have a list of known persons with different identification information (names, photographs, biometrics, etc.) and search for these persons. Identification must not be confused with verification. Verification means that a person claims a certain identity, for example by showing his passport, whereupon an official or system uses other (biometric) information to verify if the person really is the one he claims to be.

Once a suspicious character has been identified, a next step may be monitoring the identified person, or trying to influence his behaviour. That is, the monitoring and immediate action case of section 7.1 can be seen as a follow-up activity of the profiling and identification case.

With respect to profiling and identification, convergent technologies may enable new opportunities to collect and combine information. For example, converging technologies might provide new sensors to make it possible to sense brain activity and draw conclusions from it.

7.3.2 Application trends

We asked our web panel their opinion on the following statements (see Appendix B.3.3):

– People leave more and more traces in the virtual world by browsing on Internet, using their mobile phone, wearing RFID tags with them, or being observed by cameras.

– The amount of data registered about persons and objects is growing enormously.

– Passports will contain DNA based information.

– Intelligent video surveillance (face recognition) will also be possible in difficult circumstances.

All experts agree on these four statements, in particular they strongly agree on the first two.

7.3.3 Relevant technologies for profiling and identification

As already stated in section 7.1, the relevant technologies for the profiling and identification case much resemble the relevant technologies for the monitoring case. Video surveillance is more important here. Identification by using intelligent video surveillance (face recognition) is currently only possible using very conditioned circumstances (looking into the camera) and not too many persons in the database. However, out web panel (Appendix B.3.3) already indicates that active vision and opto-mechanical camera devices will allow for high-quality panning and zooming in crowds, simultaneously tracking several individual persons (faces). In this way we may be provisionally equipped with an early warning system. In the case of difficult circumstances (bad lighting etc.), there is a better chance of recognizing people based on biological motion patterns compared with face recognition.

From our literature study, as well as from expert opinions (see Appendix B), we expect the (future) technologies developments as shown in Figure 29 to be relevant for, or having a profound impact on profiling and identification. As in the monitoring case, the accent is on information technology.

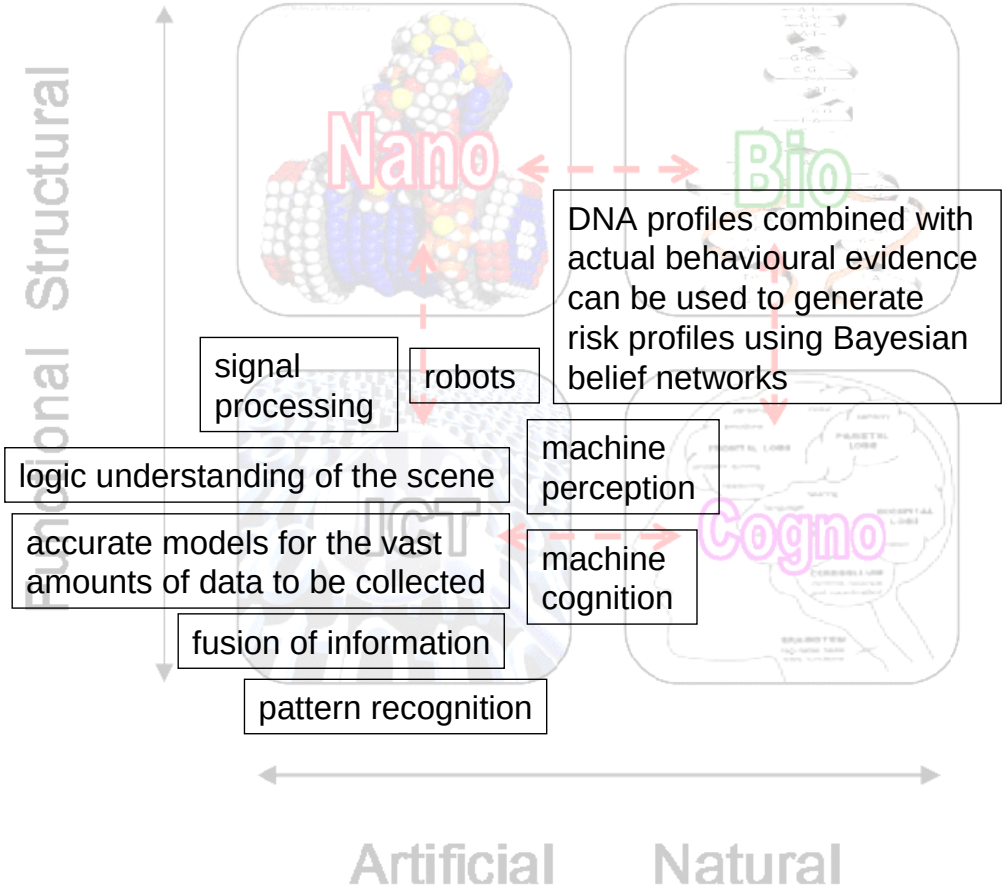


Figure 29: Main relevant technologies for profiling and identification.

From Figure 29 we observe that, even more than for the monitoring case, information technology is an important component. During the discussion in our workshop (Appendix A.5), however, the combination of several information sources has been

stressed. For example, the combination of DNA databases with fingerprint databases gave new insights and herewith a strong boost to tracing criminals. Combining many information sources or insights, which may be bio (DNA profiles) or cognition (behaviour) originated, enhances profiling. Note however that 'the last step', which is generating from all information a profile of how somebody exactly looks, is (and remains) missing.

Combining information sources might break down on organisational issues. There is much to gain, however, by integrating information islands in an international context.

With respect to face recognition, people are very good at recognising known persons (and not so good in recognising unknown persons). For machines, however, 'priming' (that is recognising persons in a crowd based on face recognition) is very difficult. Other features, however, like voice (including dialects), body, or smells can be much better identified by machines. For example, where it is difficult for human beings to identify an accent and correctly relate them to geographic areas, machines have no difficulty to distinguish Moroccan from Turkish, to mention a very simple example.

Also, much can be gained by improving models of deviant behaviour (and herewith profiling). For example, the current models of psychiatric pictures could be refined, possibly evolving into an expert system. This may take some time (10-15 years?), however.

Finally, note that using (DNA, face other biometrics) databases for profiling and identification purposes faces us with the so-called 'tourism problem'. Suppose we introduce a database system with a profile (DNA, biometrics) of all Dutchmen. Applying this system in practice means we make a distinction between Dutchmen and non-Dutchmen ('tourists'). Apart from the ethical aspects of this discrimination (see chapter 9), the example illustrates that profiling should to be tackled in an international context.

7.3.4 Expectations for the next 15 years

With respect to future forecasts, we posed our expert panel on Internet the following question (see Appendix B.3.3): 'How long will it take before the following innovations become reality?'

- Persons are continuously monitored both in the virtual and real world using ICT-, nano- or bio-enabled (wearable) sensors.
- A person's sensitivity to criminal behaviour can be derived from DNA.
- Due to enhanced man-machine (and brain-computer) interfaces, people leave so many traces that from the information stored on Internet, we know who they are and what they think.
- So-called '(remote) brain reading' can be used for profiling or identification purposes.
- Face recognition is reliable enough to be used to partly replace human intelligence

– Total information awareness: the ability to record and correlate all possible electronic traces left by a person, and the extraction of additional information, such as abnormal behavioural patterns

– Event prediction based on continuous observation of persons with an assumed security risk.

The possible answers are within 5 years, within 10 years, within 15 years, more than 15 years, and no opinion. Figure 30 shows the answers of the experts who felt themselves confident to answer this question.

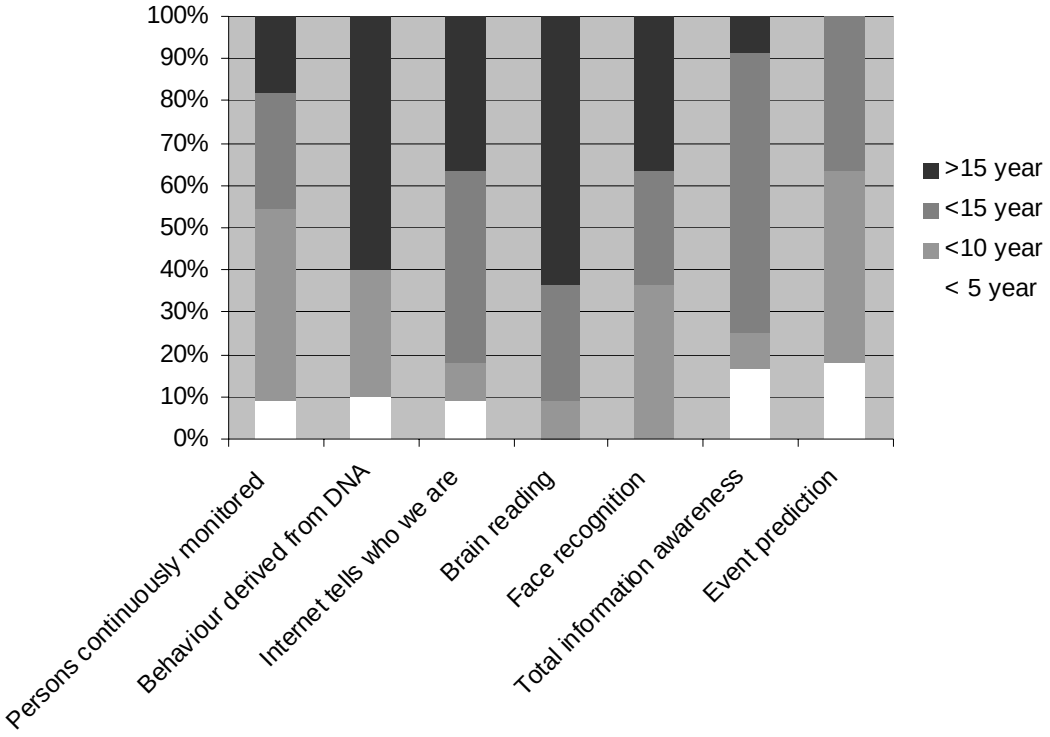


Figure 30: Expected applicability of technology for profiling and identification.

Based on an analysis of the results, we may split up the developments in profiling and identification over the following time periods. On the short or mid term (within 10 years), information processing applications are expected. Due to ICT-enabled (wearable) sensors, data about individual persons is continuously gathered, somewhere. This may lead to 'total information awareness': the ability to record and correlate all possible electronic traces left by everyone in the country, and the extraction of additional information, such as abnormal behavioural patterns. Event prediction based on this continuous observation is expected, though the quality of the prediction remains a question.

In the long term, but still applicable within 15 year, face recognition is expected to become a reliable technology to be used in unconditioned circumstances, to partly replace human intelligence. The applicability of face recognition depends on the details of the application. Nowadays, the use of face recognition for verification purposes is already common practice. Identification of individuals in crowds under unconditioned circumstances (no frontal view, 'bad' lighting, and varying outdoor weather

circumstances) has still a long way to go. Within 15 years, major advances are possible but not all expectations may come true. A second technology development that is expected to be applicable within 15 years is 'intelligence' on the Internet. Due to enhanced man-machine (and brain-computer) interfaces, people leave so many traces that from the information stored on Internet we know who they are and what they think.

Still far away and not applicable with 15 years are the so-called (remote) 'brain reading' applications. Finally, opinions differ on the ability to derive someone's sensitivity to criminal behaviour from a DNA profile. The workshop discussions concluded that it is almost certainly impossible to derive behaviour from a gene structure. Nonetheless, combining information from all kind of biosensors and cognitive analyses may make it possible to predict certain risk factors.

7.3.5 Conclusions for profiling and identification

Based on our literature study, interviews, web survey and workshop discussions, we suggest that the following applications in profiling and identification will be technically feasible by 2022:

- Widespread use of (real-time) surveillance and monitoring of humans and environments / presence of sensors in public areas.
- Unobtrusive camera surveillance and sensor networks with increasingly small sizes (short to middle term).
- Widespread use of RFID tags (e.g. in the retail sector) that can be used to track persons (short term).
- Massive databases, e.g. holding genomic information (short term).
- Coupling of databases/sensor information, improved search capabilities and artificial intelligence to logically process collected information.
- Biometrics –probably combined with other available (context) information– widely applied for security functions (but no brain reading).
- Hands-free human-computer interaction enabling input devices with fast and unobtrusive data capturing.
- Genetic screening for e.g. clinical pictures, but not for predicting behaviour.
- Secure personal data transfer, like anonymous transactions or identifier removal.

7.4 Generalising the cases

The objective of this study on convergent technologies is not to find specific technological solutions for the three application cases as described in the sections 7.1 to 7.3. Rather, this study shows the possible impact of converging technologies on the entire 'security' domain, using the three cases to focus our line of thought. Coincidentally, all three cases can be mapped on the more generic *sense-think-act* paradigm as shown in Figure 31. This paradigm may apply to many other cases in social security, terrorism or even crisis management.

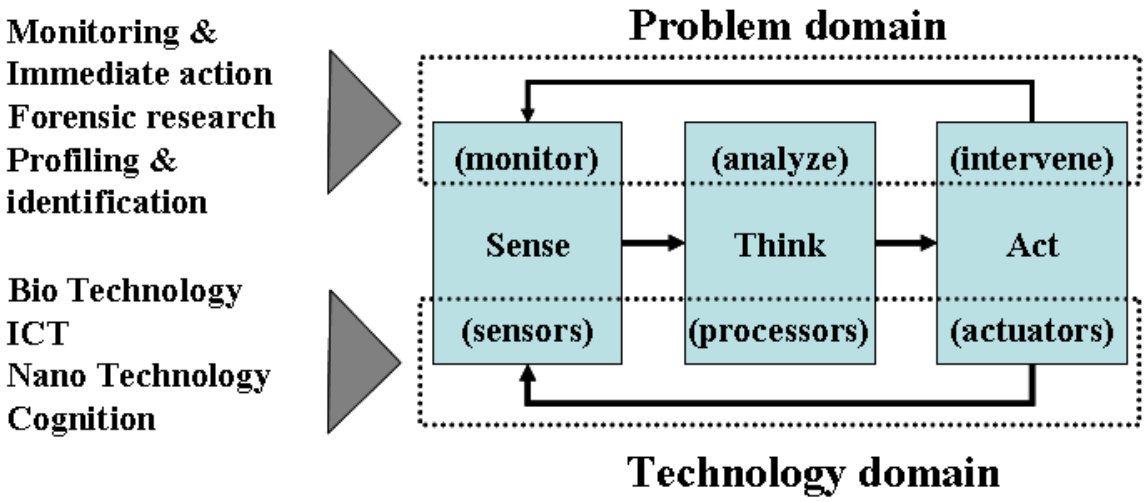


Figure 31: The generic sense-think-act paradigm.

Regarding the sensing (input), nanotechnology may enable biotechnology to develop new sensors in the body. Nanotechnology also contributes to the miniaturization and energy savings of information technology, making ICT sensors ever smaller and less battery dependent.

Regarding the thinking, information technology provides the processing power or visualization tools to use all sensor information for risk analysis and assessment.

Regarding the acting (output), information technology may enable cognitive sciences or biotechnology to regulate body or brain implants from a distance. A different way of acting, closer to the current technical possibilities, is through remote-controlled devices (such as the knee lock), or through real-time feedback from e.g. a monitoring agent.

7.5 Conclusions

We investigated which converging technologies are relevant for three cases.

- Case 1: Monitoring and following objects or persons and remote intervention in case of undesired movements and relocations (in short: *Monitoring and immediate action*);
- Case 2: Improving and developing forensic trace analysis (in short: *Forensic research*)
- Case 3: Profiling, identifying and observing persons with an assumed security risk (in short: *Profiling and identification*).

For monitoring and immediate action, currently mainly information technology is used, such as video surveillance and RFID tags. Most promising for the future seems the combination of all kinds of sensors: in the body or on the skin, brain signals and environment sensors. The impact of monitoring on privacy is important, but people seem to be willing to trade privacy for security. The technology applicable for this case resembles the technology suited for profiling and identification.

In forensic research, technology developments like lab-on-a-chip lead to changes in the process of research because analysis results steer the search for traces. Traces become smaller as well. DNA is important and has proven its value for identification. For

deriving behavioural traits from DNA, i.e. for profiling, much simpler means (compared to DNA) can be used.

Table 6 and

Table 7 summarize the relevant technologies for our application field, and the degree of uncertainty with respect to their applicability.

Table 6: Relevant NBIC technology to be applied within 15 years.

Technology	*Sensors*	*Processors*	*Actuators*
Nano	Nano imaging	Lab-on-a-chip Sprayers to find the tiniest traces	Smart materials Nano manipulators
Bio	Biosensors, biomarkers, skin conductivity, heart rate Genetic databanks	Cellular recognition Genetic analysis, DNA profiling devices	Genetic manipulation
Information	RFID, GPS, UMTS, Wi-Fi Video surveillance Web 2.0	Fast information processing, pattern analysis. Ambient intelligence	Verbal or visual message delivery, mechanical restraining devices
Cognition	Neural implants fMRI, EEG scan	Interpretation of collected neural signals in terms of intentions or actions, machine learning.	Functional electro-stimulation of brain areas

Table 7: Uncertainties in NBIC technology development

Timeline	*Sensors*	*Processors*	*Actuators*
< 5 year	Large-scale application of RFID tags Internationally coupled DNA databases Lab-on-a-chip	Simple pattern and face recognition Better and more efficient DNA analysis tools	-
<10 year	Cellular recognition Sprayers to find the tiniest traces Genetic profiling Biochemical databases	Web 2.0 (social software) 3D image of stains crime scene Contextual models for detecting aggression Real time contact with experts	Smart materials Early warning systems for behavioural derailing
< 15 year	Bio/ nano sensors Sensor networks in body	Face recognition in unconditioned circumstances Computational model human perception Portable DNA profiling devices	Miniaturisation and nano manipulation
> 15 year	Brain reading Gene passports	Quantum computing Forecasting recidivism	Electronically controlled animals Selectively erase memories Influencing behaviour by brain implants

7.6 Our expectations in an international context

So far, we sketched the developments in nano, bio, information and cognitive sciences and technologies, their convergence and their relevance for the three cases of monitoring and immediate action, forensic research and profiling and identification. This resulted in listing a number of applications that will be technically feasible by 2022 in Section 7.1.5 (monitoring and immediate action), Section 7.2.5 (forensic research) and Section 7.3.5 (profiling and identification). How do these forecasts relate to other reports?

For the beginning, the discussion on converging technologies is characterized by some very futuristic and far-ranging visions, the idea of improving human performance being the most well-known (Roco and Bainbridge, 2002). By extending the human sensors (eye) or expanding brain functions (memory and processing capacities) the human body and mind will be technically improved or the process of aging will even be retarded. These expectations seem to be more optimistic than our forecasts. In our view, two issues

have to be taken into account: practical applicability and time-scale. Renn and Roco (2006) expect the 'fourth generation nanotechnology applications' by 2020 (see Section 2.3, Figure 6). Notice however that applications working well in a lab setting still may need several years to become a commodity to be used in practice. For lab-on-a-chip technology a period of five years has been mentioned by our workshop participants. So, notice that differences in expectations may be caused by a scientific perspective in the one report (what is theoretically possible), versus a focus on practical applicability in other reports, like the one from our side. With respect to applications, the forecast from Bainbridge does not differ much from our expectations (Bainbridge and Roco, 2006: Appendix 1). The applications Bainbridge expects for 2015 are based on technologies we know from today (e.g. based on wearable sensors). Applications for 2025 include a more durable human body and sophisticated monitoring of brain activities. Most applications of cognitive sciences show up starting 2030 and the ability of scientists to understand and describe human intentions, beliefs, desires, feelings and motives in terms of well-defined computational processes is expected in 2070 (!). Also note that from the application *areas* to which converging technologies will contribute, national security is listed as the first one (2020).

Identically, our expectations are in accordance with other recent expectations, like those in the RAND report (Silberglitt *et al*., 2006), the report of the European Technology Assessment Group ETAG (2006), and the ITEA technology roadmap for software intensive systems (2004). Our time-scale resembles most the first report (which forecasts for 2020), and with the latter report we particularly agree that NBIC convergence fits in the information revolution (IT convergence). Many other reports do not focus on a technology roadmap as such, but more on application domains (Doorn, 2006; Schmidt, 2006) or research agendas (Nordmann, 2004), and in this respect provide a different perspective than forecasts based on a technology roadmap.

8 Scenarios for the application of convergent technologies in the security sector

In the previous chapters we have described the technology developments for the coming 15 years (Chapters 2-6), as well as their relevance and applicability for the three cases of Chapter 7. In this chapter we sketch four scenarios that illustrate how converging technologies can be applied in the security sector in 2022 (i.e. 15 years from now). A scenario provides a relevant, plausible and consistent image of a possible future practice. The resulting scenarios are on the one hand a means to visualise the convergence of technologies for the application domain and herewith the three cases of Chapter 7; and on the other hand they can be used as input for an assessment of the ethical, legal and social impact, as we will do in Chapter 9.

While writing scenarios, it is important to distinguish between two different drivers of change: trends and key uncertainties (Figure 32). Trends are developments, which experts signify as relatively certain. Key uncertainties are developments that are regarded as relatively uncertain.

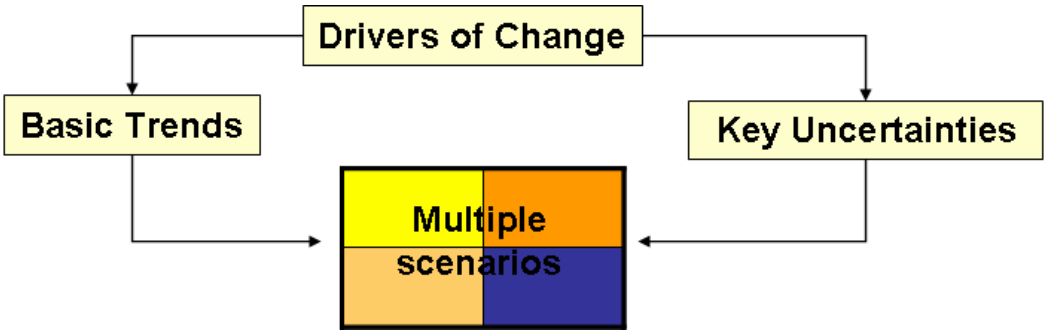


Figure 32: Process of developing scenarios.

In this section, we first discuss the basic trends for the scenarios (section 8.1). Hereafter we describe the key uncertainties (section 8.2), which allow us to define characteristic scenarios. Next, in the sections 8.3 up to 8.6, the four scenarios are provided. Each scenario describes a possible future situation after 15 years from now.

8.1 Basic trends assumed in the scenarios

The main objective of our study is to explore what can be reasonably expected within 15 years with respect to the impact of NBIC convergence on the security domain. So, primarily the aim is to sketch scenarios that are 'realistic' to happen within 15 years. However, the term 'realistic' can be interpreted from two viewpoints:

1 **A technological viewpoint**. Technological developments will be required to make the scenarios happen. Are these developments expected to be realised within 15 years? That is, we should focus on applicability in practice, and exclude all science fiction[43].

[43] Of course, though we focus on what we consider as realistic, the timing of technological (and societal) developments always remains uncertain.

2 **A societal viewpoint**. Even if a scenario is theoretically possible from a technological perspective, the required technology still (a) has to be developed and (b) has to be applied for the scenario to become reality. That is, 15 years is a long period during which societal developments may influence the development or introduction of technology.

Technology push

With respect to the *societal viewpoint*, many factors influence the speed in which innovations are diffused in society. For instance, Rogers (1995) has found that perceived innovation characteristics such as relative advantage, compatibility and complexity are a key factor in explaining the adoption rate of innovations besides the innovativeness of potential adopters, the communication channels, the social system and the change agents. Other factors include R&D budgets, hype cycles, legislation, competition, and so on. In this study it is impossible to account for all these factors. We therefore assume technology push scenarios. We focus on what is realistic from a technological viewpoint, and how this can be used by government, or how this can be used by third parties requiring a governmental reaction. Basically, this means we assume basic trends like the following:

- Citizens accept technological innovations for public security enforcement.
- Citizens are willing to trade privacy for increased public security[44].
- Sufficient resources (e.g. R&D budgets, researchers, engineers, and laboratory and production facilities) are available to develop the innovation from proof of concept to mature market application.
- Government legislation will not restrict technological progress.
- Emergence of viable business models for the technological innovations

An important consequence of this choice is that our scenarios are relatively biased to the technological possibilities. Please notice, however, that the scenarios are not meant to predict the future but are a means to facilitate the discussion on the possible ethical and juridical consequences when NBIC convergence is applied to safety enforcement. Therefore, the bias is partly handled in the ethical, legal and societal impact analysis (see chapter 9).

Still, to keep the scenarios realistic the main (basic) societal trends have to be taken into account. For each scenario we will indicate some societal assumptions.

Ambient intelligence

With respect to the technological viewpoint, the previous chapters (Chapters 2-7) have shown what is realistic or not from a technological viewpoint. Chapter 6 shows that NBIC convergence fits in the information revolution (see also Van Est *et al.*¸2006). Chapter 7 shows that our application cases all fit in the sense-think-act paradigm and that herewith information processing is important for our cases (Section 7.5). Based on these observations, the impact of NBIC convergence can be summarised as a move towards

[44] Note that other scenario studies, like '*Justitie over morgen: Scenario's en strategieën voor 2015*' (Wijck *et al*, 2007) use the willingness to trade privacy for social security as a key uncertainty. However, these scenario studies on public safety focus on social and institutional developments and their impact on safety enforcement, and pay only marginal attention to the developments in the area of NBIC technologies.

what we have labelled ‘Ambient intelligent safety enforcement’. The concept of ambient intelligence refers to a vision of a world in which technology will be integrated (invisibly) into almost everything around us, from where it will create an environment that is sensitive to the presence of people and responsive to their needs.

The most important societal and technological drivers for ambient intelligent safety enforcement are summarised in Figure 33.

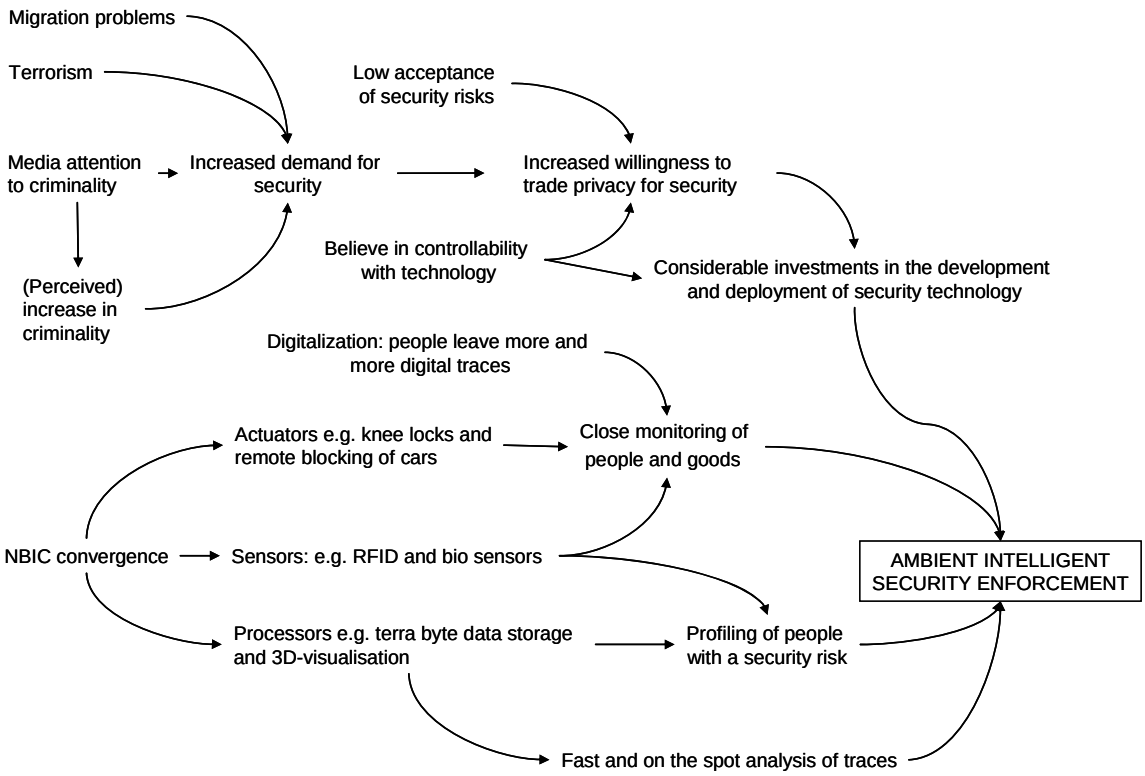


Figure 33: Ambient Intelligent Security Enforcement.

Migration problems, terrorism, (perceived) increase of criminality catalyzed by the media attention to these issues have increased the demand for social security among citizens. At the same time there is a strong believe in general that technology can increase our controllability of these security issues. Together with the increased willingness of citizens to trade their privacy for social security it induces the government and security organizations to invest heavily in the development and deployment of ambient security technology like for instance intelligent surveillance camera’s, body scan devices, etc.

This move towards ambient intelligent security enforcement is enabled by the NBIC convergence. Nanotechnology and biotechnology enable the development of new types of sensors (e.g. biosensors and optical sensing of nanoparticles). Nanotechnology also contributes to the miniaturization and energy savings of ICT sensors such as RFID chips. Information technology provides the processing power and visualization tools to use sensor information from different sources for risk analysis and assessment. Cognitive technology delivers algorithms which can be used to detect patterns in the collected data. Finally, information technology may enable cognition or biotechnology to regulate body or brain implants from a distance.

In terms of the sense-think-act paradigm (see also Figure 31 in section 7.4), key components of ambient intelligence in the safety domain are:

1 Sensors: collecting data on the behaviour of people and goods using different types (e.g. wearable, nano, optical sensors) of connected sensors (e.g. RFID, biosensors, fMRI, surveillance camera's, full body scan),
2 Processors: combining and analysing data from different sources to e.g. build profiles of people with a tendency to criminal behaviour, identify criminal suspects, and relate traces to criminal offences.
3 Actuators: acting (proactively and reactively) on undesired patterns (derived from the collected data) from real life events e.g. disturbing criminal activities, arresting criminals, fixing knee locks, closing gates.

Advances in actuator (e.g. knee locks) and sensor technology (e.g. RFID and biosensors) and the fact that people leave more and more digital traces enable the close monitoring of people and goods and remote intervention in case of security risks. In addition, new processor and sensor technology enable profiling of people with an assumed security risk. Finally, advances in processor technology like lab on chip technology and 3D visualizations of crime scenes enable the fast and on the spot analysis of traces.

Together these technical and societal developments enable what we have labelled Ambient Intelligent Security Enforcement. Security technology is integrated (invisibly) into almost everything around us enabling a shift from reactive authorities, collecting information and evidence to be used on purpose, towards a proactive government, using technology to anticipate on and prevent crime.

8.2 Key uncertainties

Based on a literature review, expert interviews and the expert workshop we have identified important technological developments in the areas of NIBC and assessed them in terms of maturity in 5, 10, and 15 years (see Figure 25, Figure 27, and Figure 29 in chapter 7). In discussing these technological developments and the application cases with external experts we noticed that the realization of the vision of ambient intelligent security enforcement is hampered by two key uncertainties:

1 The degree of *information sharing* that can be realized between stakeholders involved in security enforcement like police, intelligence agencies, forensic research units, department of justice, citizens, public service bodies, etc., on a national and international level lags behind the necessary levels. Ambient intelligent security enforcement can only be achieved if one succeeds in swiftly combining information from different sources (cameras, internet, phones, observations, sensors, etc). This requires that one is able to couple the different information systems and facilitate the information exchange between experts. The degree of information sharing that can be realized is influenced by the organizational structures, cultures, work processes and information systems of the different organisations involved. Depending on the absorptive capacity and attitude of these organisations this may take little or more time.

2 The degree of *information processing*: the capacity to store and analyse the collected data. The ability to store data grows faster than the ability to process data. Many researchers predict a data explosion and expect a decentralisation of data storage and

processing. The bottleneck is except for battery technology[45] not so much the hardware (e.g. processors, storage) but the software and human brain power needed to devise algorithms to analyse the terabytes of data on persons and objects. A single human genome, for instance, is already 6 Gigabit of data. New computing paradigms and pattern recognition algorithms are required to deal with these vast amounts of data. Although a lot of 'low hanging fruit' in this area (e.g. analyzing facial expressions) experts regard for instance, quantum computing and a computational model of human perception as necessary components in the a long term while they are currently far from feasible.

'The ability to store grows faster than ability to process. Who's going to eventually evaluate? We have a limited attention span, we need to sleep and rest. The capability to do all kinds of processing, data storage and data transport are exponentially rising. The bottle neck will therefore not be the hardware but the software. It will be more complex in order to handle that data explosion. Writing the appropriate software does not progress nearly at the speed of the progress in hardware. The solution would therefore be to do more in hardware. This may be one way out.
The ability to extrapolate is hampered by the way we think. When a new thing comes on our desk then we can imagine it. Application software seems to be the bottle neck. How to program? We may need 10 million programmers and we may have technology make the programs. But still we need humans to do the integration.
Software is a big issue. It is amazing that the coming ten years all progressing lines like Moore's law are probably just going on. Even if not you will still see a continued exponential growth through 3D chips and other clever innovations as extra factors to add some margin. There is already enough in store for 10 years of exponential growth. The challenge will be to use this power with care to prevent us all drowning in data.'

Interview with prof.dr. John Long (TU Delft)

To conclude, the experts agree with the basic trend of ambient intelligent safety enforcement. Important uncertainties or bottlenecks in realizing this vision are the degree of information sharing and the degree of information processing that can be realized in the next 15 years. We treat these factors as key uncertainties to construct four future scenarios of social security enforcement (see Figure 34).

[45] Power management is progressing quite rapidly but signal processing is often power hungry. Circuit technology is expected to follow Moore's law (number of transistors on an integrated circuit for minimum component cost doubles every 24 months) for another ten years; in contrast improvements in battery power are expected to be rather incremental.

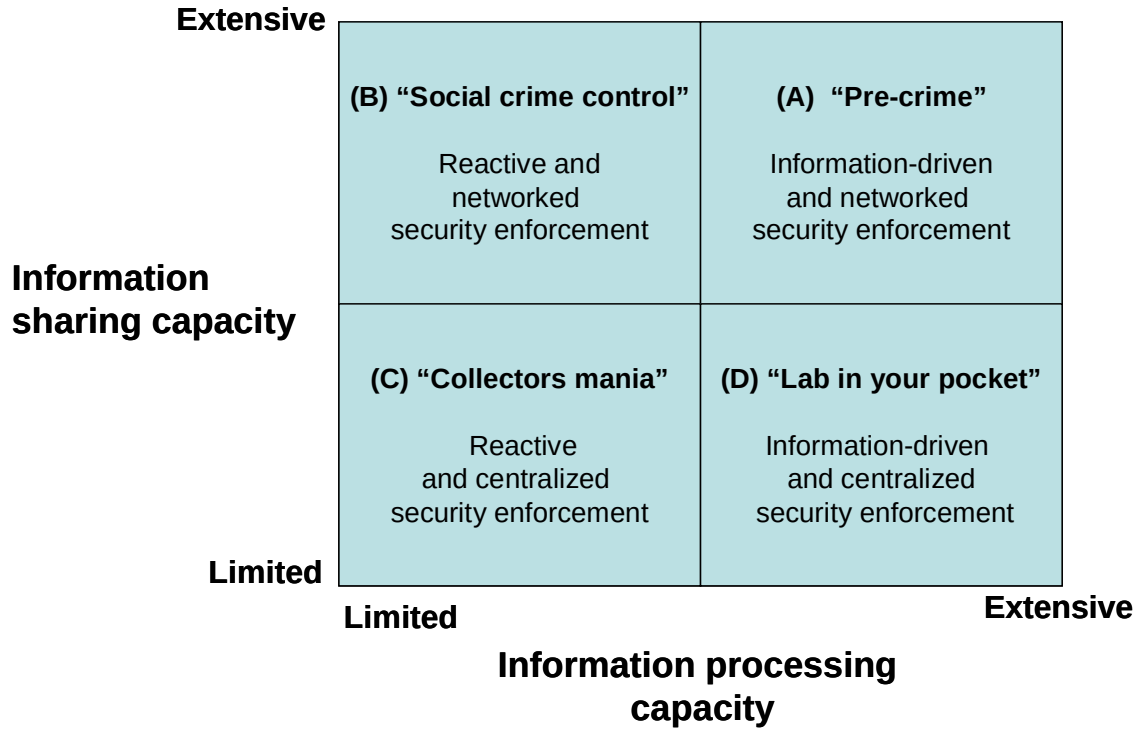


Figure 34: Using two key uncertainties to build four 'related' scenarios.

The scenarios will be elaborated in the following sections. With respect to the relationship with the cases as described in chapter 7 (i.e., monitoring and immediate action, forensic research, and profiling and identification), each scenario contains elements of each of the three cases. In this way, we emphasize the generic character of this study and we use the fact that the cases have generic features as well (see section 7.4). This also means that different aspects of a particular application case may be 'distributed' over the different scenarios. Nonetheless, being commissioned to focus on three specific cases, for each scenario we have chosen a 'primary case', which might make the scenarios to a certain extent application specific.

8.3 Scenario A: Pre-crime

The 'pre-crime' scenario is the most 'futuristic' in the sense that it assumes the convergence at the most, as far as we can imagine. Of course, the scenario is still judged to be technologically realistic for the period up to 15 years from now. At the same time, the scenario assumes a high degree of organisational collaboration, which requires changes in 'culture' compared with nowadays organisation. Enabled by the extensive information sharing and processing capacity security enforcement is moving from after the fact finding suspects and collecting evidence to proactive and preventive security enforcement.

Table 8: Main characteristics of the 'Pre-crime' scenario.

Title:	*Pre-crime ('De misdaad voorbij')*
Societal assumptions:	Citizens accept technological innovations for public security enforcement and are willing to trade privacy for increased public security
Key technologies used:	<5 year: RFIDs, Pattern and face recognition in video surveillance, crowd control <10 year: Web 2.0 (social software), Real time contact with experts, Contextual models for detecting aggression, Early warning systems for behavioural derailing <15 year: Full computational model human brain functions, Miniaturization and nano manipulation (preventive medicine) >15 year: Quantum computing, new computing paradigms
Main application case:	*Profiling and identification:* Profiling of individuals or groups, as well as advanced pattern analysis make it possible to (real-time) anticipate on crime events
Relationship to other application cases:	*Monitoring and immediate action:* From a video analysis, the distinction between kidnapping and voluntarily entering a car can be made (to be used for monitoring and protecting persons applying for asylum). *Forensic research:* Profiles (including DNA profiles) can be used for forensic research. Due to prevention – less forensic research is needed.
Storyboard:	This scenario shows a shift from a reactive towards an information-driven proactive environment. Sensors are available everywhere and the information can be processed to take the right decisions. The government policy is anticipation on and prevention of criminality. Characteristics of the future situation are: – Persons with an assumed security risk are monitored – The widespread use of RFID tags in de body for monitoring and identification purposes – The use of sensors (video surveillance, body sensors, brain scans, etc.) for e.g. aggression detection – The coupling of public and private information sources for an all-embracing analysis of a person's behaviour and relationships – Actuators that restrict persons in their movements

A video surveillance camera in a shopping centre has detected an anomalous behaviour: a nervously looking person who tries to repress his apparent fear without immediate cause

for acting this way (no life threatening situation). What kind of person is this? Is it a person close to a nervous breakdown, a student before a difficult exam, a thief pursuing his next victim, or even a terrorist planning a suicide attack? To rule out options the surveillance systems automatically requests the video recordings of other cameras (from other organisations) that have captured the same individual, such that his itinerary is reconstructed up to one hour earlier.

One camera shows that 35 minutes ago the person used an ATM. The transaction recorded by that machine is then correlated with other transactions performed with the same debit card up to three months ago. Additional videos become available, many of them showing the person accompanied by a known criminal. What is the relation between these two persons? Are they acquainted? What are they up to? It is now decided that both persons should be closely investigated on a personal level. Research shows that our nervously looking person has recently travelled a lot. Also, during the last weeks he has bought relatively many aspirin tablets, which may indicate a health problem. At the same time, his housemates buy more alcoholic drinks in the supermarket as the average Dutchmen, which may be a pointer towards an addiction problem. Therefore, the observer decides to take action.

The surveillance system activates a private body scanner at the end of the street when the suspect enters its active area. Unfortunately the public scanner is not of any use because our person under surveillance uses an RFID guard that prevents reading tags as well as has a so-called second layer of armoured skin which makes our suspect's body to be invisible for that sensor. However, this does not necessarily make the person more suspected. Such systems are a commodity and their use by our suspect could be expected, because some months ago he has been a victim of an RFID surprise attack (criminals using RFID scanners to find persons which carry expensive equipment or many bank notes). Also, no explosives or weapons are detected. No alarm is therefore raised, but the person's alarm status is raised to 'orange'. This means the person, who uses his implanted RFID chip for authentication to, e.g., start his car, enter a bar, etc., is partly restricted in his movements; as well as is followed for a while by the next cameras on his route for the rest of the day.

The observations of that day are stored in a database, which contains records of people who have behaved strangely and are considered a security risk. People who are tagged as a 'security risk' are permanently monitored and security forces are alarmed when video and voice recordings seem to point to criminal behaviour. Based on the persons behaviour of today it is likely that he is innocent, but nonetheless the observer decides to pay the person a visit and ask him about his relationship with the convicted criminal. For, he has been monitored unobtrusively and by visiting him he knows he is being observed and, in case he really strays from the right path, he may mend his ways.

8.4 Scenario B: Social crime control

The 'social crime control' scenario assumes a high degree of information sharing and a low degree of information processing capacity. Security enforcement is decentralised with a high degree of collaboration and information sharing. This allows to accurately monitoring the movements of a limited set of goods and persons with an assumed security risk. An important bottleneck is the processing of data collected by devices such as surveillance cameras, body sensors, and DNA analysis tools. As a consequence the police encounter problems with responding swiftly to emerging security risks.

Table 9: Main characteristics of the 'Social crime control' scenario.

Title:	*Social crime control ('Onderling veiligheidstoezicht')*
Societal assumptions:	– People reject the idea of life long imprisonment of people at her Majesty's pleasure (the Dutch 'TBS') and believe in the idea of re-integration – People have a lot of confidence in the controllability that can be achieved with technology
Key technologies used:	<5 year: RFIDs, knee lock actuators, pattern and face recognition in camera surveillance, tracking and tracing, both outdoor (GPS, GSM, UMTS, UWB) and indoor (RFID, WLAN). <10 year: Web 2.0 (social software, Contextual models for detecting aggression, Early warning systems for behavioural derailing <15 year: Power scavenging, body sensors (nano, bio, cognition) and body actuators (drug delivery)
Main application case:	*Monitoring and immediate action:* Persons can be monitored individually, for example prisoners under 'house arrest' are monitored (tracking and tracing) very extensively resulting in a virtual prison.
Relationship to other application cases:	*Profiling and identification:* Intelligent camera surveillance and identification of persons.
Storyboard:	Due to collaboration with private partners or citizens, small-scale, individual monitoring is possible close to someone's home environment in this scenario. Characteristics of the future situation are: – Individual tracking and tracing of persons with a seamless handover from outdoor (GPS) to indoor (camera surveillance) or public to private systems – Entire population is assessed for tendencies to criminal behaviour – Blurring borders between virtual and physical behaviour – Citizens participate in tracing criminals and law enforcement; mutual observation and social control of citizens

Jaap is on treatment for paedophilic behaviour in *Second Life* and his suicidal tendencies. Fortunately, the current observation techniques enable an accurate diagnosis and individually tuned treatment for his problems. Recently, like all eight-year old children in school, his son has even been observed for his tendency to criminal behaviour. This early prevention programme combines all available knowledge from biosensors, cognitive models and behaviour observation. His son, however, is a good soul and will never end in the mess Jaap has got in. But for Jaap, the medicine and the behavioural and therapeutical programme he is on have produced promising results. Individual

observation of his behaviour in detention and on Internet fine-tuned his treatment and for the first time since years he is allowed to go on probation leave for the weekend.

He is intending to visit his parents. He has got clear instructions from his therapist where he is or is not allowed to go. He is now on his way to buy the groceries he needs to cook for his parents. However, he is not aware that in the past year a new elementary school has been built close to the supermarket he is about to visit. Fortunately for his own security and the security of others, Jaap has been equipped with a body sensor monitoring his physiological state and a GPS transmitter which allow monitoring Jaap's whereabouts. Since within buildings the signal strength is too weak to track Jaap, intelligent surveillance systems, which are now obligatory for all public places, take over the indoor tracking.

Not suspecting any problems, Jaap is about to cross the street in the direction of the newly built elementary school. The eye tracking software detects that he –already closer than 400 metres from a risk object (the elementary school) – is looking at the new building. Immediately the security system activates the knee lock and the most nearby security agents are alarmed to look for Jaap on the video surveillance systems. Since Jaap is already in the middle of a busy street, which he judges as a very dangerous situation in case his knee is being blocked, he has no other choice than pressing the emergence button. Immediately, the knee lock is released, but also the front gate of the elementary school is sealed off to prevent anyone to enter the playing ground where children are now enjoying their 15 minutes break. Moreover, a selected group of registered civilians gets an SMS message with a case description (paedophile on leave approaching school) and pointers to the location and Jaap's photograph. They belong to the group of civilians participating in the 'prison without walls' project.

Jaap is getting frustrated and upset because he can not imagine what he could have done wrong. He also gets nervous because a young girl gazes upon Jaap. She may be one of the civilians of the 'prison without walls' project, but on the other hand she is very young and does not take action according to the protocols Jaap is aware of. Jaap does not know she is an applicant for asylum. Being a potential victim of lover boys or slave-running, she is under the governmental protection programme and also got the SMS message. Meanwhile, Jaap's body sensor detects an unhealthy adrenaline level and releases tranquilizers to keep him calm for the time being. After a few minutes, police officers are at the spot who gently and unobtrusively take him in for questioning.

8.5 Scenario C: Collector's mania

The 'collector's mania' scenario assumes a limited information processing and sharing capacity. The different government bodies that are involved in public security enforcement find it difficult to collaborate and exchange information. Due to the difficulty of getting access to information of other government bodies the centralised intelligence body has built its own (shadow) databases to be not so dependent anymore on those of others. The scenario may be regarded as the current situation extrapolated into the future with organisational and technological concepts being kept unchanged (though modernised, of course). Therefore, this scenario may be seen as a reserved variant and none of the three application cases has a favoured position.

Table 10: Main characteristics of the 'Collector's mania' scenario.

Title:	*Collector's mania ('Verzamelwoede')*
Societal assumptions:	– Civilians play an active role in social security enforcement – Civilians doubt the effectiveness of public social security institutions and start arranging for their own security
Key technologies used:	<5 year: Better and more efficient DNA analysis tools, International coupling of DNA databases, RFIDs, Pattern and face recognition in video surveillance
Main application case:	None
Relationship to other application cases:	*Monitoring and immediate action:* camera surveillance *Forensic research:* lab-on-a-chip trace analysis *Profiling and identification:* Participation of civilians in identifying criminals
Storyboard:	This scenario extrapolates the current, somewhat reactive (rather than anticipatory) processes towards the future. This does not mean, however, that the scenario is less advanced because the NBIC technologies still advance. Characteristics of the future situation are: – Much information is collected, arranged, presented etc. In particular, the data is used for searching afterwards. – Tasks shift from public partners to private partners (services) and eventually to civilians, but more on a service rather than collaboration base. – Enhanced camera surveillance, e.g., it is possible to distinguish voluntary or forced behaviour

An alarm is raised by the camera surveillance system in the public shopping centre near the railway station. Suspicious behaviour has been detected that matches the 'kidnapping profile'. Immediately, video images are reviewed. Indeed, someone is drawn into a car. Further rewinding, however, shows the person has arrived with the same car 15 minutes before and meanwhile visited the electronics store. The cameras in the shop show some expensive apparatus has been taken away and apparently (electronically) detagged by a shop-lifter.

Fortunately, this electronics store also sells all kind of forensic sensor apparatus that have become a commodity. The policemen taking notice of the incident are overloaded with the newest stuff, though available to the police as well, not being purchased by their department, of course. With the help of these apparatus, including a DNA profiler and nanosensors that can identify the geographic origin of traces, the thief can be identified. For, wearing a hood and carefully not looking into the cameras, the face recognition alone has not been sufficient in this case. Having identified the shop-lifter, actions can be taken.

Rob walks with his pregnant girlfriend in Amersfoort when he receives a message on his mobile phone alerting him that a shop-lifter is on the loose in the district they are strolling. He receives a description of the thief and is asked to call the police when he has more information. The message contains a picture taken from one of the surveillance cameras in the shopping mall that has been robbed. The face resembles a person which lives in the neighbourhood he and his girlfriend are living. He calls the police and tells them that he thinks the suspect is living in the Dollard Street close to where they live. Although he does not know the exact address the police officer on duty is very grateful for this information.

Early next morning Rob sees the suspect walking in fast pace to the railway station. He grasps his phone and notifies the police immediately. Meanwhile Rob sees that the man is behaving strangely. It looks as though he is trying to break in to a car. On request of the police officer on the phone Rob starts recording what he sees. It excites him that he is collecting evidence for the police. Two minutes later the policemen are on the spot. The man is caught and hand-cuffed.

Satisfied Rob walks home. Unfortunately, he is caught spitting his chewing gum on the pavement. The surveillance camera of the bank immediately responds by giving him an official warning using the built-in loudspeaker. A bit annoyed, Rob quickly leaves the spot.

8.6 Scenario D: Lab in your pocket

The ‘lab in your pocket’ scenario assumes an extensive information processing and limited information sharing capacity. The different government bodies that are involved in public security enforcement find it difficult to collaborate and exchange information. Despite of these difficulties the way of working of forensic research has changed drastically. DNA samples are now analysed on the spot and hypotheses and experts are involved much earlier in the process. The re-organisation required for this new way of working was a major operation. The scenario may be regarded as the current situation extrapolated into the future with organisational and technological concepts (mobile lab facilities) being changed and technology is becoming available to civilians and criminals as well.

Table 11: Main characteristics of the 'Lab in your pocket' scenario.

Title:	*Lab in your pocket ('Laboratorium in je broekzak')*
Societal assumptions:	Believe in the effectiveness of crime scene investigation
Key technologies used:	<5 year: Better and more efficient DNA analysis tools, International coupling of DNA databases, lab-on-a-chip <10 year: Web 2.0 (social software), sprayers for finding tiny traces, biochemical databases, 3D images of stains at the crime scene, real time contact with experts <15 year: Portable DNA profiling, devices combining DNA information with 'soft' information, bio- and nanosensors >15year: Gene passport, quantum computing, new computing paradigms
Main application case:	*Forensic research:* The process of forensic research being thoroughly changed due to technological possibilities on the place of crime (quick analysis), current functional phases are mixed.
Relationship to other application cases:	*Monitoring and immediate action:* The use of video surveillance systems. *Profiling and identification:* face recognition and DNA profilers are used for identification purposes.
Storyboard:	This scenario has been based on (trace) analysis tools becoming small, quick, accurate and handy. Herewith their results steer the (forensic) research process. Also, these tools become a commodity and therefore are used by private researchers (or criminals) as well. Characteristics of the future situation are: – Nano sprayers to detect the smallest traces – 3D reconstruction of crime scene – Lab-on-a-chip technology available to everyone – Global sensor information becomes available to citizens (tracking locations, camera data, etc.) – Real-time analysis of data, e.g., for database matches, trace analysis, etc.

An unknown person has been found dead in a café this morning. The victim has been in the café the entire afternoon but all visitors and personnel of the café claim to have seen nothing. However, from the position of the body and the nature of some inflicted body wounds, hardly possible by falling to the ground the police officers suspect an unnatural death. Blood of the victim is analysed using lab-on-a-chip technology for proteomics, metabolites and trace elements to determine the mental and physiological state of the victim close before the incident. Was the victim stressed, ill, or aggressive? The tests show the presence of a virus and biotic potential that are fatal within two hours. So

something must have happened in the café and in consequence an elaborated forensic research is performed.

Given the public nature of the crime scene it will be a tough job to discern crime-related traces. The crime scene investigators start analysing the traces using their mobile lab facilities. Sensors are sprayed over the crime scene to build a network that instantly analyzes the traces over an area of 50 m^2. 25000 human traces are detected. A 3D image of the crime scene is digitally re-constructed which outlines the position of the body and the found traces. A quick pattern analysis, which combines information of past similar crime scenes with the found traces, shows that only 47 may be related to the events at the crime scene. All but the 47 sensors bound to the relevant samples are deactivated. A selective retriever collects only the active sensors, extracts the samples, and places them on an array of DNA profilers.

Meanwhile, a local correspondent has started his own investigation. On the spot the surveillance cameras, which are now obliged in all cafes and viewed by a private regional service centre, are consulted for deviations. Unfortunately the crime itself is difficult to see on the cameras; however, the cameras provide a good overview of who has visited the establishment on the last 24 hours. All 74 visitors could be identified using a combination of face recognition, context information (most of them can be traced on Internet, where people voluntary upload their location[46]) and questioning witnesses. Checking their records shows that three of these visitors appear to have a criminal record. One of these visitors has a history of violence and two of the visitors have been tagged before as security risks, yet as far as can be detected were not convicted of a crime.

The 47 different traces are communicated to the attorney's office to request an identification order. Within 5 minutes the crime scene investigators receive an approval to run the traces through the DNA database. 8 matches are signalled with 2 visitors of the café. The addresses of these 2 persons and their families are revealed and the closest police agents are alerted. They will be questioned. At the same time the first hypotheses on the way the victim could have died are discussed with forensic experts using video conferencing. The local correspondent, however, persists in his research. He claims that criminals have scattered around deceitful traces and requests a second opinion on the traces by the independent nano-forensic lab. They are specialised in small traces and may detect traces on the traces proving that the traces have been moved from elsewhere. The results of this counter research are not yet made public, however.

Finally, the asbestos and nano removal services are allowed to clean the crime scene that has been polluted by the nano spray.

[46] Like www.bliin.com

9 Major trends and social and normative impact assessment

This chapter focuses on a number of possible social and normative, i.e., moral and legal, trends which condition the impact of converging technology developments. Rather than taking the new technological options as the unique source of eventual impacts, we should recognize that impacts are always co-produced by the interactions of groups of actors including, for instance, producers of technical products, technical and social scientists, policy makers and nongovernmental organizations (NGO's). This chapter starts with trends in society, which will be modulated and perhaps shifted by the emergence and uptake of converging technologies. Thus, it is complementary to the earlier chapters.

The trends were chosen because they were deemed important for the use of converging technologies for law enforcement – the central theme of this report. 'Big Brother' predictions, focusing on privacy, have drawn critical attention for a long time; and with every technological advancement (and interest to exploit it), there has been a new wave of concern. The scenarios, laid out in Chapter 8, suggest further issues. This chapter focuses on several possible social, moral and legal trends that may come along with the developments described so far. The social trends are primarily concerned with implications of increasing polycentric and multi-actor crime surveillance and challenges to governability. The normative ones focus on new privacy concerns, issues of self-control versus control by others, the moral foundations of law and the legitimacy of new forms of regulation. It should be noted from the outset that these trends – individually and as types – will practically often overlap and intertwine. In order to highlight possible salient developments, it is, however, useful to distinguish them *in abstracto*.

As our world changes, our normative outlook can be expected to change as well. Some examples in the description of the trends indicate how this works. We will conclude with some considerations about what has been called co-evolution of new technology, society and normative outlooks.

A methodological *caveat* should be made. It is difficult to identify the impacts of new and emerging science and technology, and particularly of converging technologies, as we can currently only speculate about their eventual shape. The four scenarios, described in Chapter 8, were built around two main drivers: the extent of information sharing and the capacity of information processing. Each of the two drivers could take different forms, enabled by converging technologies, depending amongst others on the extent and nature of uptake of technological options. For example, there may be reluctance to exploit new possibilities for information sharing and concomitant processing, because of considerations of organisational autonomy, and/or to respect privacy. The example of the relatively problematic issue of RFID tagging of products, from producers to customers, and in retail shops, shows that uptake of new technological possibilities does not happen automatically.

Our approach with regard to the impact analysis and assessment is one of several possible alternatives. Whichever one might choose, one has to be careful of what Alfred Nordmann has called the if-and-then syndrome: 'An if-and-then statement opens by suggesting a possible technological development and continues with a [possible] consequence that [if realized] demands immediate attention. What [may] look like an

improbable, merely possible future in the first half of the sentence appears in the second half as something inevitable. And as the hypothetical gets displaced by a supposed actual, an imagined future overwhelms the present' (Nordmann, 2007). We projected a certain future technological performance, in order to consider possible impacts. And in discussing such impacts and assessing them, we are forced to reify that technological future, as if it would be there, somehow, without further discussion.

The implication is that a discussion of social, moral and legal impacts, here of converging technologies, will have an exemplary character rather than offering a picture of the future world. Still, this can draw attention to issues and challenges that deserve to be paid attention to in the here and now.

9.1 Social impact

9.1.1 Trend 1: Shifts in data collection and processing

As the scenarios indicate, converging technologies enable an enormous increase in data collection and processing, which is occurring already as we write. Not only are data stored in ever more databases (e.g., Google, customer databases, social networking, e-community sites, loyalty schemes, CCTV images), but also, new types of data have appeared, such as location data (mobile phones), Internet surfing data, identification data (RFID), and DNA data (like geographic ancestry), that traditionally were not generated or processed. Moreover, it has also become much easier to process and use data, through digitisation, automated recognition, data sharing, and profiling. Increasingly, data collection can also take place unobserved (aerial photography, miniature cameras, directional microphones, micro sensors, 'smart dust'), using more senses than sight and sound (olfactory sensors, chemical 'cameras'). Much of this is not new, but the scale of data increase and the combination of all developments lead to a truly qualitative increase in the data 'out there' about citizens and their personal lives.

A recent trend is also that legislation is passed to *mandate* the storage and processing of data, for fear of the data disappearing before they can be used by the government for law-enforcement or national-security purposes. Examples are the preservation order (Art. 16 Cybercrime Convention, implemented in Art. 126ni, 126ui, 126zja Dutch Code of Criminal Procedure (hereafter: DCCP)) and the Data Retention Directive (2006/24/EC), which mandates telecom providers to store all traffic data for a period of 6 months to two years (a Dutch implementation Bill is currently pending in parliament). These data, stored for government purposes, may then also be used by the private parties storing them, and perhaps be shared with other third parties as well, as long as they comply with the relevant legal framework for data processing (like the Data Protection Act and Chapter 11 of the Telecommunications Act).

Almost all of these data, both the 'emerging' data and those mandatorily stored, can, if legal conditions are met, be accessed and used by the government for law-enforcement and intelligence purposes. Both the judiciary and the intelligence services have comprehensive powers to order delivery of data or to gather data themselves (see Koops, 2004: 79-119, 194-213; Vedder *et al.*, 2007a: 23-32 for an overview). However, most of these powers are currently still to a significant extent related to indications of specific crimes being committed or planned. This is in line with the 'Lab in your pocket' scenario, but the 'Pre-crime' scenario moves beyond that through its data collection occurring independently from specific crimes. Also, the 'Collector's mania' scenario significantly extends current legal practice by its large-scale collection of data, without

too concrete purposes of using them in specific cases. The Data Retention Directive sets a precedent for this, but still has the difference that the data are being stored by private parties rather than collected and stored by the government itself.

The result of this trend – today and possibly even more so in the future along the line of the 'Collector's mania' and 'Pre-crime' scenarios – is that not only are more and more data being created, but also, they are disseminated much more widely to a larger number of parties, access to data is made easier for the government, and control over these data is becoming increasingly difficult for data subjects. The consequence of this trend is that, even with the same investigative powers, governmental authorities are in a position to collect and use significantly more data about citizens than before, and this increase is not only quantitative but also qualitative. This in turn enables the government, in principle, to know better than ever before what citizens, including criminals and terrorists but also 'the man in the street', are doing. Also, in the very long term, several NBIC developments might lead to potential control of citizens in ways previously unimaginable, for example, by influencing the brain. (The normative discussion of such a possibility can easily fall into the 'if and then' trap, so the technical as well as social difficulties of actually realizing such a possibility must be kept in mind).

A combination of the trend to have increasing data-processing capabilities and the trend to focus on prevention (see section 9.2.2) entails that the 'footprint' of criminal law and intelligence is slowly widening to cover an increasing part of society. This is a key finding in the larger development of what social-science scholars have termed a 'risk society' (Beck, 1999), a 'surveillance society' (Lyon, 2002), and a 'culture of control' (Garland, 2001). These various perspectives contribute to an image of a risk-averse society that, in order to control risks and prevent damage, uses large-scale monitoring in all sectors and spheres of society (cf. Murakami Wood, 2006). Crime control is *the* central element of such a society: 'the new crime control developments (…) play a role in *creating* that [late modern] world, helping to constitute the meaning of late modernity. Crime control today does more than simply manage problems of crime and insecurity.' As Garland phrases it for America and Britain today, '"late modernity" is lived – not just by offenders but by all of us – in a mode that is more than ever defined by institutions of policing, penality, and prevention.' (Garland, 2001: 194) Also in the Dutch context, some scholars have argued that criminal law seems to have become a first resort in society: for every risk and every problem, criminal law is being looked at as a logical instrument to address it. This constitutes a paradigm shift from the traditional role of criminal law as an *ultimum remedium* (Koops, 2006: 26-28; Klip, 2004: 1).

The implications of the shifts in data processing are not limited to control of crime, however. Data can be accessed and used by the government for other than law-enforcement purposes, for example in controlling compliance with administrative law (tax law, environmental law, etc.), or in providing personalised services in the context of e-government. Larger-scale use of data for a variety of government applications is facilitated by increasing identification of citizens, including an overall cross-sectoral ID number like the Dutch BurgerServiceNummer. Such applications have advantages, like increased efficiency and ease-of-use, but also disadvantages, like less autonomy and less privacy for citizens (cf. Koops, Buitelaar & Lips, 2007).

Given the technical complexity of converging technologies being applied for a variety of law-enforcement purposes, a further effect will be the increase in information that private parties will have about citizens. Private parties with relevant expertise on the technologies will, in public-private partnerships or independently, develop and perhaps

apply several of the technologies at hand, which means they may get access to many more data than they currently have. An example is RFID tags: if certain types of RFID tags are important for certain law-enforcement applications – like crowd control in the 'Pre-crime' scenario – then not only government, but also industry and retailers selling the products containing these RFID tags have access to the data generated by the people carrying them. Like traffic data retention enables telecoms providers to store and data mine more data of customers, and 'know-your-customer' laws result in financial service providers collecting more data from their customers, so RFID technology might enable clothes stores, phone sellers, and/or soccer stadium operators to know more about their customers or visitors.

To what extent converging technology applications for law enforcement, and their spill-over into other applications, actually will enable other parties – other sectors of government and private parties – to know more about individuals will depend on the laws and technical and organisational architectures devised for these applications, partly because of concerns about uncontrolled knowledge. This illustrates the non-linearity of impacts. For example, if technological performance in this area is strong, there will soon be breaches of privacy, and the outcry about them can lead to stricter regulation and changes in the architecture of the technology. If, on the other hand, technological performance stays weak at first, there will be little or no concern, attention will shift to other issues – and the gradual improvement of performance will be less visible, as will the increasing use of data by the variety of partners. So, counter intuitively, the eventual impact may well be larger. Such shifts in the co-evolution are a challenge for impact assessment, and a reason to use scenario approaches, particularly when these are enriched by understanding of social and normative trends.

9.1.2 Trend 2: Shifts in methods of surveillance

Surveillance, whether through data collection and processing or in whatever other way, is not just a means to a goal, like surveilling criminals or crowd control. It embodies an overall move towards more disciplining in our societies, and reinforces it. We have already mentioned the debates on the 'surveillance society' and 'culture of control'. The Pre-crime scenario and the Social crime control scenario are pointing to new methods of crime surveillance with implications like the ones that have been addressed by Bentham and Foucault. Bentham's ideas of a Panopticon, in his discussion of a prison, are important because they build on the centralising of control that technologies can offer, making individuals increasingly more visible with limited possibilities of verification of observation (Gordon, 1986; Lyon, 1993; Spears and Lea, 1994; Tomkins, 1998). Recently, potential panoptic effects of nanotechnological applications have been highlighted by Mehta (2002, 2003) and Van den Hoven and Vermaas (2007).

Described by Bentham as 'a mill for grinding rogues honest' (see, Bentham 1843), the Panopticon prison project involves the construction of a central observation tower in a transparent and hemispherical building, which serves to employ constant surveillance exercised simultaneously by a single guard. To reduce cost, Bentham conceived of the Panopticon prison as a privately operated institution. The Panopticon prison is furthermore meant to stimulate self-discipline of the inmates. It is construed as a one-way observation system in order to force prisoners to follow prison regulations. Even without the actual presence of a gazing guard, the power effects of invisible monitoring can be felt by the inmates. In the Panopticon prison, uncertainty is used as a means of subordination (Lyon, 1993: 657). As a consequence, despite the absence of institutionalised physical violence, the constant gaze, or, at least, the suggestion of the

constant gaze, induces normalising effects on conduct, self-perception, personality, and world view (Mehta, 2002: 31).

The idea of obtaining normalising effects by (the suggestion of) the constant gaze is one of the basic assumptions of the widespread practices of camera surveillance. Present day speed cameras induce speed limiting behaviour in motorists, even if they do not contain or are not connected to a storage device. These examples show the centralizing thrust of disciplining through surveillance, even if there is no central observation tower anymore as in the original Panopticon. Similar effects can be expected from the surveillance systems described in the Pre-crime scenario and the Social crime control scenario. For example, knowing that there could be cameras monitoring their action can cause people to change their behaviour.

Foucault's writings illuminate potential 'panoptic' implications of modern surveillance technologies. They expand Bentham's thought with a broader concept of government and governmental rationality, which seem to be crucial to converging technologies development. In *Discipline and Punish: The Birth of Prison* (1977) Foucault elaborates on Bentham ideas to illuminate his key concept of discipline. According to Hunt and Wickham, this concept paves the way to deal with the complex ways in which power is inscribed in the construction and use of technologies (1994: 20). Foucault conceived of discipline as the distinctive form of modern power. He identified the existence of a whole complex of techniques of power that do not rely on force and coercion. Discipline deploys not so much punishment but a mix of micro-penalties and rewards. It is characterised by hierarchical observation, and it operates through norms, normalising judgements, through tiny, everyday, physical mechanisms, by systems. According to Foucault, the chief function of disciplinary power is to train and to 'make' individuals (1977: 170). Individuals are treated both as objects and as instruments for its exercise. Behaviour is also changing in the context of increasing self-control. The implications of this shift in methods of surveillance, however, must also be related to an emerging culture of visibility. In a context of accepted transparency individuals could experience surveillance as usual business and feel no desire to change their behaviour.

'Governmentality' is another key concept in Foucault's work that can illuminate the impact of new surveillance techniques. Governmentality refers to a governmental rationality, which involves a calculating preoccupation with activities directed at shaping, channelling and guiding the conduct of others (Gordon, 1991). The production, dissemination and utilisation of knowledge and information become central in governmental intervention. In Foucault's terminology, government is not only an activity of institutional and quasi-state bodies. He stresses the dispersion and privatisation of disciplinary power. The gaze of authority has been decentralised, supplemented and displaced by surveillance techniques of indirect observation.

The point of this extended discussion of Bentham and Foucault is that it alerts us to impacts which are not derived from a specific technology, but from a host of technologies which all fit an overall trend towards disciplining, and reinforce this trend. Impact assessment should then not focus on one or another technology, but on the overall pattern and how it is being reinforced.

9.1.3 Trend 3: Shifts in power relations

The spread of converging technology applications, particularly their increasing 'autonomy' (from passive to active devices, and on to 'smart' systems') and their

miniaturisation and commodification that make them available to a wide range of users, will reinforce two trends in socio-technical power relations. First, because the possibility to delegate regulation to technology, by incorporating norms and their enforcement in technical devices (see also section 9.2.3) will be greatly expanded. Second, because the state monopoly on such disciplining will be changed. Of course, there is a strong speculative element in assessing such impacts, but bits and pieces are visible already.

Clear examples of delegation to technology can be found in the social crime control scenario. One can also see wider impacts: If criminals (or more neutrally, detained people) can mingle freely in the outside world – because their creating mischief is blocked – new ways of 'seeing' or judging them may arise. The knee-lock device might come to be considered as not essentially different from active driver's assistance devices, which can block the driver's move to change lanes if it sees a car in the new lane. If such devices (these are just two examples) become common, people might also start to rely on the technology to look after them, in order to prevent them from creating mischief. This is a double delegation: First, there is reliance on the effectiveness of the technology (and thus on its quality and its maintenance), and second, the definition of what is 'mischief' now lies with the designers and producers of the device.

Converging technologies may also contribute to the decentralisation and privatisation of regulation and law enforcement. As the technologies treated in this report will develop, the knowledge, skills and expertise to understand them may further specialise. This means that supervising the developments and closely watching for instance the incorporation of legal norms and enforcement in technology will become gradually more difficult. (Supra-)national and international governmental organisations may find it unattractive to take up these responsibilities and relocate them again to private parties, i.e. the parties that themselves develop the technologies or especially established parties or for instance NGOs that may monitor the developments (Vedder *et al.*, 2007b).

The incorporation of regulation and its enforcement in technology may change the citizen's perception of the state and his position in society. The transformation that may take place here has to do with the citizen's relation to the authorities and powers that were traditionally assigned to the state. Were these hitherto concentrated in the state and the various government organizations, now the citizen will have to get accustomed to a situation in which these authorities and powers are more and more assigned to manifold and disparate parties, ranging from the traditional state government, to international organizations, private parties, to NGOs, and, of course, the citizens themselves.

The transformation, described so far, may have interesting effects in terms of participatory democracy. It, however, also raise a further question: Can there be some quality control of the new practices, can they even be pro-actively influenced? Which actor(s) could carry such a responsibility, and, if so, under what conditions? Answering these questions and organizing solutions should preferably be an international undertaking, since converging technology is by its very nature a border-crossing phenomenon. There may be a tendency to look to the level of supranational government (e.g. EU) and to international organizations (e.g. UN and WTO). But this might not work, partially because of lacking expertise and other practical barriers and partially because of long existing reservations to power transfer powers from the national to the supra- or international level in the field of criminal law, even if there are clear functional arguments for such supra- or international governance.

Take again the case of criminal law enforcement. This is still to a substantial degree considered a national issue. Although, for instance, the influence of the EU on member states' criminal law systems is increasing, nations are still reluctant to hand over responsibility for law enforcement to a supra-national level. For applications in converging technologies, this means that often, for each new application in the sphere of law enforcement, discussions have to take place and agreements have to be made among EU member states for facilitating cross-border use. Mutual access to DNA profiles in national forensic databases (cf. the Prüm Convention), cross-border computer network searches (cf. the Convention on Cybercrime), and technical protocols for wiretapping (cf. the ETSI ES 201 671 and ETSI-NL standardisation procedures) are examples that illustrate how slow, complex, and piecemeal such supranational discussions and decision-making are. For applications like crowd control based on RFID tags (pre-crime scenario) or prisoner-tracking through GPS (social crime control scenario), this means that such applications will likely be restricted to the national context first, reducing their effectiveness, and that cumbersome procedures will have to be followed to enable cross-Europe(an) applications. Also, there is a significant risk that law-enforcement technologies developed in the Netherlands are not, except with high costs, compatible with applications in other countries.

Broader impacts of delegation to technology and decentralisation/privatisation of governance, as outlined above, cannot be influenced in any simple manner. As with the trends discussed in 9.1.2, recognizing and assessing them, and making sure such understanding is widely available, will make actors more reflexive, and hopefully, lead them to make better choices.

9.1.4 Trend 4: Changes in governability

We have moved from assessing impacts (co-produced by general trends and converging technologies) to issues of governability of such developments already in 9.1.3. The regulation of converging technologies themselves may confront us with specific problems of governability. These have to do with the uncertainties as well as promises and concerns involved in converging technologies and with the path dependencies of technological development (see, Dorbeck-Jung, 2007, 2008).

A study of the International Risk Governance Council highlighted the increasing uncertainty, complexity and ambiguity of nano-technological (and nanotechnology-enabled converging technologies) risk problems (IRGC, 2006). An important point is their distinction between more articulated issues, in their case, first-generation nanotechnology with 'passive' sensors and materials, and the uncertainties and complexities of later generations of nanotechnology. For the first generation, professional risk/impact assessment can be done. For the later generations, with their uncertainties but also their more active (and thus disciplining) features, deliberative approaches would be necessary.

Other governability issues arise from undesirable path dependencies of technological developments. Technological developments can get locked-in into a particular direction of development so that other, more desirable options are excluded (Rip, 2006). The classic example of path dependency is the QWERTY arrangement of keys on the keyboard of typewriters (in Anglosaxon countries), which continued after the original reason (controlling the speed of typists so as to avoid having the hammers get entangled) had disappeared. In the area of ambient intelligence (with a service orientation and/or monitoring and control), path dependencies might well occur, linked to promises of huge profit-making (Whitman, 2006). Under the umbrella promises of ambient intelligence, a few areas with vulnerable subjects (the elderly, the handicapped, the criminals) are

getting special attention. Technologies and practices of usage developed in these areas may set directions, already because of the effort put into dedicated improvement of performance. Given the experience of earlier path dependencies, which became ungovernable, the challenge is to identify incipient path dependencies, assess their further evolution and impacts, and find ways to modulate them at an early stage, before the actual impacts have appeared.

This challenge of governability of new and emerging science and technology is increasingly recognised, and approaches like constructive technology assessment have been developed to address the challenge (cf. Rip and Te Kulve, 2007). Converging technologies are more complex (and uncertain). Still, tendencies can be identified which can then be taken up in constructive technology assessment. The key governability point in such approaches is that the interest is in creating/stimulating processes in which possible impacts can be deliberated and actors can modify their choices and strategies accordingly.

9.2 Normative impact

9.2.1 Trend 5: Shifts in privacy concerns

Privacy is one of the central moral and legal issues that have been raised in the debates of the impact of converging technologies. Privacy and data protection have been discussed at large in relation to applications of information technologies. Applications of nanotechnology (i.e., invisible tags and sensors) may give rise to new privacy concerns that are different from the traditional privacy issue. Decentralization, unobtrusiveness of surveillance and extension of the parties that can have access to personal data may become of vital importance

It should be noted, for instance, that converging technologies may contribute not only to the centralization, but also to the decentralization of observation and surveillance. Miniaturization and commodification will further enhance the availability of observation and surveillance devices to the general public. Consequently, the private life of citizens may become a subject of scrutiny not only by governmental organizations and private organizations, but, more and more, by fellow citizens.

The privacy effects of decentralised use of personal data may become just as important as the panoptic effects of central databases, which have shaped the privacy discussions since Foucault referred to Bentham's prison project (Van den Hoven and Vermaas, 2007). With RFID tags the unobtrusiveness of surveillance becomes a major privacy problem. Regarding new sensor devices, the privacy discussion may be taken back to the level of the design of the artefacts that help to generate information. The extent to which converging technology applications for law enforcement actually will enable public *and* private parties to know more than presently allowed about individuals will depend on laws and technical and organisational architectures devised for these applications. Particularly in the technical, functional, and organisational design process, choices could be made to restrict third-party use or re-use of data for other purposes than originally intended.

9.2.2 Trend 6: Shifts in the focus of criminal law

In Western legal systems, the main general objectives of sentencing have usually been presented as: retribution, deterrence and rehabilitation (Harris, 2007: 306-348). These objectives are based on interests of society (protection, peace, prevention, restoration, compensation etc), as well as on interests of the offender (dignity, protection). In current criminal law the focus lies on the offender (Zippelius, 2003: 134) with lately a modestly

growing interest for victims. Recently, the attention seems to shift to interests of society, deterrence and retribution. Converging technologies have the potential of reorganising the fight against crime and terrorism. Rather than being restricted to damage control – finding and punishing perpetrators – damage *prevention* becomes a focus for law enforcement.

This shift from reaction to prevention is, of course, clearest in scenario A through its emphasis on 'pre-crime'. It is, however, also a substantial element of scenario B, in the monitoring of convicts in 'prisons without walls' and using actuators like drug delivery to prevent them from escaping and committing new crimes, and, of course, in the 'Collector's Mania' scenario with its emphasis on large-scale collection of data.

This trend is not unrealistic: it has already been at work in the past decade and is continuing to the present day. Law enforcement and surveillance are taking place in earlier stages with a focus on prevention and early detection of crime (Koops, 2006: 18-28; Borgers, 2007). Examples can be given in substantive law: preparatory acts have been criminalised in the 1990s (Art. 46 Dutch Criminal Code (hereafter: DCC)), recently also for computer crimes to the extent that storing a password which someone intends to use for hacking is punishable with up to one year imprisonment (Art. 139d para. 2 DCC). Likewise, new types of activities have been criminalised, like bomb hoaxes (Art. 142a DCC), scheming for terrorist crimes (Art. 114b, 120b DCC), and plotting a crime by a single person (Art. 46 DCC, as amended in 2002), which emphasise early intervention by law enforcement. Even more important, procedural law has been adapted to enable investigation activities in an early stage: special investigation powers can be used without probable cause, in case of 'indications' of a terrorist crime (Art. 126za et seq. DCCP), and suspects of terrorist crimes can be held in preventative custody under relatively loose conditions and for a long period of up to two years (Art. 66 para. 3, Art. 67 para. 4 DCCP).

The shift has also been facilitated by legislation to mandate the storage and processing of data, for fear of the data disappearing before they can be used by the government for law-enforcement or national-security purposes. Examples are the preservation order (Art. 16 Cybercrime Convention, implemented in Art. 126ni, 126ui, 126zja DCCP) and the Data Retention Directive (2006/24/EC). This Directive sets a clear precedent for large-scale data-collection without concrete purposes for specific use. Interestingly, the data are being stored by private parties rather than collected and stored by a government body itself (see also subsection 9.1.1).

The strategy embraced by the Dutch Council of Chief Superintendants of Police focuses on 'information-driven police care' (*informatiegestuurde politiezorg*), which includes, among other things, large-scale use of technology, monitoring of groups of potential suspects rather than of individual suspects, and a primary focus on prevention (Projectgroep Visie op de politiefunctie, 2005). According to the Council, the Dutch police should use a large number of innovative, non-criminal enforcement strategies, varying from frequent controls at infrastructural intersections in large cities, targeted controls at hotspots, and structurally signalling and passing on information to other government agencies than the law enforcement sector. Through monitoring streams of information and potentially suspect people, criminal acts can be noticed at a very early stage, preferably before they are actually committed.

This strategy of information-driven police care has been articulated as a vision by the police sector, and as such has not, or not yet, been embraced by the legislator. However,

the trend of strengthening crime prevention using other means than law enforcement is visible in numerous recent regulatory measures: preventative frisking in 'safety risk areas' (*Staatsblad* 2002, 420), a general duty for citizens aged 14 and older to identify themselves (*Staatsblad* 2004, 300), and administrative orders to persons 'who can be related to terrorist activities or terrorism support' not to visit certain places or parts of the Netherlands, not to come near certain persons, or to report regularly at the police (Bill 30 566, currently in the First Chamber).

In short, the 'Pre-crime' scenario's focus on prevention fits in with current trends in law-enforcement and national-security measures. However, it should be noticed that the scenarios move significantly beyond current measures: although the criteria for intervention are being lowered, currently, there usually still is some indication of potential wrong-doing at the individual level, based on concrete circumstances. The 'Pre-crime' scenario's focus on large-scale group profiling and monitoring allows a much wider distance between the time of monitoring and possible intervention and the time where the supposed criminal activity is normally expected to occur. The criteria for monitoring and intervention also seem significantly broader than is the case currently.

In the Dutch context, some scholars have argued that criminal law seems to have become a first resort in society: for every risk and every problem, criminal law is being looked at as a logical instrument to address it. This constitutes a paradigm shift from the traditional role of criminal law as an *ultimum remedium* (Koops, 2006: 26-28; Klip, 2004: 1). In contrast, Foucault's analysis of the importance of discipline and governmental rationality ('governmentality') results in another conclusion. This is the expulsion of law (Hunt and Wickham, 1994: 50). According to Foucault, law comes to be 'colonised' by the new disciplines being invaded by practices of observation and training. Other underpinnings for the diminishing role of law can be derived from the promises of immense profit-making that are expected from CT applications. As other technological developments show, these expectations may put legal aspects on the background of governance.

9.2.3 Trend 7: Shifts in the conceptions of freedom and responsibility

With the use of converging technologies, efforts are being made to gain further insight in the human mind and the functioning of the brain. According to the Western systems of criminal law, criminal liability requires the criminal act (*actus reus)* and the element of a guilty mind (*mens rea*) (Harris, 2007: 306-348). The commission of criminal acts must be shown to have been done *voluntarily*, *wilfully and knowingly.* For these reasons, someone committing a prohibited act while in a state of unconsciousness, acting like a robot, will normally be excused because the act is not the outcome of the accused's rational will. People are held liable for their actions and decisions, because they do have a moral choice to make. There may be exceptions to liability in concrete cases, but this is the general rule. It is important to note here that the notion of free will underlies the very system of modern criminal law (Remmelink, 1995: 12-13):

> in criminal law, which directs itself with its norms at man who is, in principle, free, human will plays such a decisive role (…) [O]ur [Criminal] Code is unmistakeably built on this indeterministic underlying principle – man is a homo volens.

Freedom of the will is generally considered to be one of the basic assumptions for holding people responsible or accountable in law and morality. At least at first sight,

attributing guilt and blaming people do not seem to make much sense when people do not have freedom of the will, i.e., cannot but do what they do. Supporters of the concept of free will assert that every human being can exercise control over his or her actions and decisions. The question whether and in what way people control their own actions and decisions is closely related to questions on freedom and causal determinism. Causal determinism holds that human behaviour (including mental states, such as thoughts and intentions, and actions) can be explained completely as a part of a causal chain ruled by laws of nature.

If causal determinism would be true, it would at first sight raise serious questions on how, and to what extent, individuals can be held morally accountable for their actions and decisions. Determinism asserts that every decision and action is a certain and unavoidable result from previous states of affairs. According to many determinists, when a person acts, this act was necessitated by antecedent conditions. These conditions cannot include conditions that were themselves not necessitated by other preceding conditions as the idea of free will seems to imply. A person cannot be held morally accountable, as he had no alternatives. In the eyes of a determinist, punishing a murderer is not an act of holding him accountable, but simply a way of dealing with crime – and this would be something that was actually already predetermined as well. This is not just a general philosophical discussion. The application of converging technologies, e.g. those involved in brain stimulation, for example for Parkinson patients and for depression, appear to build on, and thus reinforce a causally deterministic view.

Causal determinism has always met with criticism. Many of the opponents adhered to the freedom of the will and either denied determinism by bluntly insisting on an inexplicable element in the choices of persons, or tried to show that determinism in the end does not undermine the freedom of will that is needed for morality. The latter view is referred to as *compatibilism* (Vivehlin, 2003).[47]

Scientific research, e.g. genomics, nonetheless, appears to be building on causal determinism. For example, further advances in genomics want to show that particular behaviour (or at least, propensity to such behaviour) is caused by particular genes. Hence, the behaviour could be considered unavoidable and beyond the scope of accountability. This does not prevent intervention, though, such as locking up dangerous persons for the safety of themselves and others.

This is a superficial picture, however. Geneticists, now agree that behaviour is almost always influenced by multiple genes, interacting in complex ways, and in interaction with environmental factors. An example of what has sometimes been coined a 'crime gene' is a gene that controls the activity of an enzyme called monoamine oxidase (MAOA). People who carried a version of the gene linked to low levels of MAOA

[47] Supporters of compatibilism state that determinism and free will are in fact compatible. The main arguments of compatibilists are directly or indirectly inspired by Immanuel Kant's classic distinction between the phenomenal and the noumenal world, i.e. the natural world and the world of freedom. They come in a linguistic and a metaphysical version. According to some compatibilists, the language of determinism is mainly descriptive, whereas the language about free will is mainly prescriptive. Although the two are of course in many ways connected, according to these compatibilists, they are mutually irreducible. Other compatibilists, such as Dennett (2003) and Wolf (1993), accept determinism full-heartedly as they refuse to assume that some kind of uncaused cause could be effective in human behaviour. They define free will not as the ability to choose and act independently of any prior cause, but as the ability to make certain choices on the basis of one's own general values and principles, without being forced to do so by other persons or circumstances, and to act upon these choices without hindrance by external barriers.

production were much more likely to indulge in anti-social behaviour such as violent crime.[48] The gene itself is not the cause of anti-social behaviour, because many other factors, both biological and social, also play a role. As a result, no genotype can be said to 'cause' certain behaviour. What is more, even if a certain genotype were found to be substantially linked to, for example, aggression, this only indicates a *propensity* for aggression, but not a causal factor for aggression in concrete cases. As a result, even the famous but rare 'aggression gene' found by Brunner et al. (1993) in a Dutch family cannot exculpate a bearer of this gene for a concrete murder: he still would have had sufficient opportunity to choose differently (if only by avoiding to end up in situations where he knows that he would become excessively aggressive).

In addition to the relationships with causal determinism there are other ways in which converging technologies may affect the issue of free will. Risk profiling, for instance, may affect the options of the individuals involved. Not by undermining the existence of free will, but by merely restricting the range of options for choosing and acting (Custers, 2004). In the compatibilist's view and in the views of many who deny physical determinism, free will implies the ability to make certain choices on the basis of one's own general values and principles, *without being forced* to do so by other persons or by circumstance. In cases where converging technologies limit the number of options, the *technology forces* individuals in their choices. For a more detailed account on how information technology forces people in their views on others, see Solove (2004).

Limiting the range of options may influence the behaviour of individuals in specific ways. Technologies such as data mining and profiling may result in confrontation with unwanted information (Custers, 2004). For instance, when group profiles are used for early diagnosis or the prevention of disease, it is possible that people in risk groups be approached with a warning. In this way, people are confronted with their health prospects, without having requested to be given such information about themselves. Especially in the case of very negative group profiles, such a confrontation may have a large impact on people's lives. Apparently healthy people may be confronted with the fact that they may only have a limited amount of time left, which may upset their lives and the lives of others. In some cases, people may prefer not to know their prospects while they are healthy. In fact, the Dutch Civil Code gives patients the right not to receive certain information if they do not want to (Article 7:449 BW) (Nouwt, 1997). These problems may become even greater when little or no treatment is available. Obviously, such knowledge about themselves may influence the behaviour of individuals. For instance, people may feel they have no options left ('nothing to lose') and act differently than they would have done without such knowledge.

Converging technologies will be part of this general dynamic, but may also increase the number of options in some cases. New materials may provide a wider range of functionalities of human implants, increasing body functions and thus the range of possible behaviour. Due to new communication technologies, people may get in contact with people they would have never met otherwise. Knowledge and data are easily disclosed to individuals looking for particular information.

There is an additional impact: converging technologies may influence the quality of choices that are being made. For example, information and communication technologies

[48] http://news.bbc.co.uk/1/hi/health/2165715.stm

disclose much more information than ever, and people exploit the new options, for example in finding out about medical treatments and discussing these with their doctors. On the other hand, the abundance of information may confuse people (particularly non-experts). The same can be said for the awareness of consequences individuals may have of their actions and decisions: on the one hand converging technologies may be extremely sophisticated in predicting the consequences of a particular action; on the other hand, there may be so many consequences that it is hard to decide which action is best.

In sum, converging technologies may influence our conceptions of individuals, individual identities, particularly regarding their freedom of will and their responsibility. These influences may be for better and for worse. Positive effects would be, for instance, the availability of more information, of advanced technologies to widen the range of options and of more sophisticated predictive models to support actions and decisions. However, these effects may also have negative aspects, for instance, when overview is lacking over omnipresent information, when the range of options is narrower than technologies suggest and when sophisticated predictive models get self-fulfilling prophecy effects. It may be expected that converging technologies will further enable the possibilities to predict and influence human behaviour. Self-control and personal responsibility will more often than currently be substituted by control by others and paternalistic interference The concept of criminal liability may need some adjustment with regard to the conception of the criminal act and the guilty mind. The idea of freedom of the will as currently used in law and morality, however, need not be abandoned..

9.2.4 Trend 8: Norms and their enforcement

Many of the applications of converging technologies will enable a combination of the stages of establishment and enforcement of regulation. Traditionally, norms and the means to enhance the observance of those norms – e.g., sanctions and penalties – are two separate things. Generally, people have some choice either to follow a rule or not. If they do not follow the rules they run the risk of having sanctions imposed on them. That risk may motivate them to follow a rule, but it does not *force* them to do so without leaving any other option open. In other words: the traditional nature of law in which norms and their enforcement are separate leaves people some room, some freedom to act according to the law voluntarily. (Of course, already now norms and enforcement are incidentally and on a small scale combined, e.g. in round points and road bumps in traffic law, and in so-called digital rights management for compliance with copyrights.)

If the possibilities of combining norm establishment and norm enforcement will be realised with regard to certain parts of the law – for some reason it is difficult to imagine that all of law can be completely incorporated in technologies influencing behaviour – citizens will automatically abide with the law in these fields. They will be traceable everywhere they go, their emotions and intentions or at least their external behaviour will be surveilled and analysed and subsequently influenced with the use of actuators in order to prevent deviance. There might even be no need to know the parts of the law involved anymore.

It is interesting to reflect on this possible development from two perspectives. These perspectives are not brought to the fore in order to morally evaluate the development, but rather to highlight possible changes in the general normative outlook on the one hand and

possible transformations in views on the governance and regulation regimes on the other hand.

9.2.4.1 Moral outlook

The first perspective that we would like to draw attention to is the one of the dissolving analogy between morality and law concerning the practical divide between norms and enforcement.

The traditional separation between norms and enforcement in law mirrors the loose connection between norms and sanctions in morality. In certain views of morality, particularly those of (neo-)Kantian and religious, e.g. Christian, denominations, – views that have been and still are very influential in many Western societies – this is considered to be an all-important and intrinsically valuable characteristic of morality: it leaves room for freedom for choosing either to observe moral rules or not to do so (see also the previous subsection). This freedom to take up responsibility in turn is considered as an important characteristic of being human. In (neo-)Kantian and Christian ethics, the emphasis on the importance of freedom and intention even entails that actions that are performed non- or involuntarily, cannot be qualified as morally right or wrong or as moral at all, for that sake. Although other conceptions of morality, such as consequentialist ones, do not present similar views explicitly, the assumption that freedom of choice to act morally right is at once a necessary precondition for morality and intrinsically valuable seems to be widely spread.

Seen from this (neo-)Kantian or religious angle, closing the gap between norms and enforcement in law separates law from morality by taking away the freedom of choice between right and wrong. In the Kantian perspective, imposing a system of law in which norms and enforcement are closely intertwined is an offence to a human being, because it does not take him seriously as a morally autonomous subject. For both the Kantian and the Christian, acting within that system would be morally indifferent, trivial even. This changes the nature of law: no longer is it a morally-inspired collection of norms and rules that should guide people to behave well (normatively, like not killing, and/or functionally, like driving on the right side of the road) in society. Instead, law becomes a set of morally-neutral, unavoidable obligations for people to behave 'well', and 'well' in this sense loses its normative meaning and is restricted to a functional interpretation.

Now, of course – as will be more extensively reflected upon in the section about the normative framework – it might be the case that one will find reasons in the Christian and (neo-)Kantian perspectives to influence the transformations in the nature of law in which the technological developments may result. Alternatively, the technological developments and the resulting transformations in the nature of law may also alter the (support for) the general moral outlook in which freedom is deemed a valuable precondition of morality, thus giving way to for instance a more thoroughly consequentialist moral outlook (compare Vedder, 2001).

9.2.4.2 Legitimacy

Closing the gap between norms and enforcement may bring about important changes in the division of powers with regard to legislation and enforcement. This, in turn, may make it necessary to pose questions regarding the legitimacy of the emerging regulatory regimes. Inescapable enforcement by technology entails pushing back the interference by police, prosecutors and magistrates. Most likely, private parties – because they have

more knowledge of new technologies than government officials usually have and because they develop and deploy the new technologies – will play an important role in undertaking the incorporation of legal norms and their enforcement in technology. In a sense private actors will take over parts of the tasks of public parties such as the legislature, magistrates, prosecutors and the police (Leenes and Prins, 2006). From the point of view of legitimacy, one may want to question this shift and to see the movement accompanied by requirements that guarantee that something similar to the traditional conceptions of the rule of law is safeguarded.

In addition, it should be noted that tying up norms and enforcement in technology changes the possibilities of supervision and correction. Enforcement through technology mostly means that conformity to the norm is inescapable. What should happen, however, if the norm is wrong or incorporated in the technology in the wrong way, so that people following the norm will not do the right thing (Leenes and Prins, 2006). What can be done if the norm is unjust or has been incorporated in technology in such a way that its application is unjust? As long as the norm and the enforcement are separated, people can refuse to act upon the norm and try to justify their refusal before a judge. Where norm and enforcement are united, this possibility will fail them. This could make it all the more important to address requirements regarding the justification of the norms that are incorporated in technology and regarding the accuracy of the whole process of incorporating norms and enforcement in technology.

9.3 Conclusion and Prospect

Eight possible social and normative, i.e., moral and legal, trends may condition the impact of the use of converging technologies for law enforcement:

1 Shifts in data collection and data processing: More and more data are being created; they are disseminated more widely, to a larger number of parties; access to data is made easier for the government, and control over these data is becoming increasingly difficult for data subjects. The consequence of this trend is that, even with the same investigative powers, governmental authorities are in a position to collect and use significantly more data about citizens than before, and this increase is not only quantitative but also qualitative. This in turn enables the government, in principle, to know better than ever before what citizens, including criminals and terrorists but also ‘the man in the street’, are doing.

2 Shifts in methods of surveillance: Increasing possibilities of surveillance will induce more normalising effects on conduct, self-perception, personality, and world-view, than ever before.

3 Shifts in power relations: Regulation will be delegated more from persons to technology and from public, governmental parties to private organizations and citizens.

4 Changes in the governability of technologies themselves: Growing uncertainty and complexity will increasingly complicate the governance of the emerging technologies and their applications.

5 Shifts in privacy concerns: As new possibilities of observation and surveillance show both centralizing and decentralizing tendencies (that do not mutually neutralize each other) and instruments for observation and surveillance become increasingly unobtrusive, both the perception and nature of privacy invasions will change.

6 Shifts in the focus of criminal law, away from reaction, retribution and rehabilitation, towards prevention and risk control.

7 Shifts in the conceptions of freedom and personal responsibility: These may affect the ways in which persons perceive their own and others' identities; they need not automatically undermine conceptions of morality and law that take personal responsibility and free will as their starting points.

8 Growing fusion of norms and enforcement: The inclusion of norms in technology that influences behaviour will involve increasing challenges to moral outlooks in which the free choice to act morally or legally right is primordial and new challenges regarding the legitimacy of arrangements for regulation and enforcement.

As the world changes, normative outlooks can be expected to change as well. Some of these changes have been indicated in the description of the trends. It is nonetheless important to note that the trends could also be seen as explicating a necessary additional element in the scenarios. Impacts occur in context, and are co-produced through technological developments and social and normative developments. Impact assessment has to take this into account, up to the further possibility of normative outlooks changing in the course of this co-evolution.

If we combine the scenarios (and their background considerations) with our present discussion of trends, we see as one of the key issues (and trends, and challenges) poly-centric governance, particularly in relation to infrastructures. The maintenance and use of ambient intelligence / surveillance systems requires a plurality of actors, each with their responsibility and accountability (cf. the Dutch tradition of water management, but also transport infrastructure). Among them, there are now also private actors, partly because of the competence of existing private actors in producing and servicing, partly because of new position and roles emerging (an example would be how point-of-care sensors and actuators, embedded in hardware and software offering help to individuals: call centres or their equivalents then become necessary to handle queries, and shift requests for confirmation of diagnosis to the right people).

A key general challenge for the future will then not be about government actors, but with the role of private actors and their accountability. Including down-to-earth issues of liability, and thus reluctance of private actors to take on larger responsibilities. With regard to accountability and regulatory capture lessons can be drawn from the current discussions in public governance (May, 2007). More individualized scenario items, e.g. of individuals arranging their own security ('Collector's Mania' scenario), will still depend on competent advisers, and delivery and maintenance. Just as with markets and competition, there will be a need for government oversight of the arrangements.

There is a general role of government vis-à-vis new and emerging technologies as well: to stimulate exploration and exploitation of new and emerging science and technology for what they can do and mean; but also to set boundaries to such developments because of possible negative impacts and the opening up of further, possibly undesirable developments (the 'slippery slope' argument which drives prohibitions and moratoria, cf. Swierstra and Rip, 2007). This dual role is sometimes managed by dividing it over different government departments (e.g. a Ministry for Trade and Industry pushing new technology, and a Ministry for Environmental Issues keeping it in bounds). But the tension and trade-offs remain.

Here, co-evolution returns, now of technology, society and normative outlooks, including the expectations that norms and values might shift (see Swierstra and Rip, 2007). Normative outlooks with respect to new technology and its uptake and impact are not given, and there may be deliberate attempts to move them in certain directions. The patchwork of issues around crime control, surveillance, agency, autonomy and the role and nature of law where converging technologies will enable certain developments as well as constrain others, could become subject to such deliberate attempts. Consideration of normative outlooks is sometimes narrowed to issues of mere public acceptance. Our discussion of normative trends can be used to counteract, or at least mitigate, such approaches.

10 Conclusions

In this study we investigated the impact of converging technologies on the security field in general and on monitoring & immediate control, forensic research, and profiling & identification in particular. We have observed that the advances in nano, bio, ICT and cognitive technology and sciences are large. Moreover, these technology fields increasingly converge. Convergence is defined as a synergetic combination of two or more provinces of science and technology.

The convergence of nano, bio, ICT and cognitive technology enable what we have labelled 'ambient intelligent security enforcement'. Both nano- and biotechnology enable the development of new types of sensors (e.g. biosensors, fMRI). Nanotechnology also contributes to the miniaturization and energy savings of ICT sensors such as RFID chips. Information technology in turn provides the storage capacity, interconnections, processing power and visualization tools to use sensor information from different sources for risk analysis and assessment. Cognitive technology delivers algorithms which can be used to detect patterns in the collected data. Finally, information technology may enable cognition or biotechnology to regulate body or brain implants from a distance. In this world nano, bio, ICT and cognitive technology will be invisibly integrated into almost everything around us. Data will be collected on the behaviour of people and goods using different types of small and connected sensors. This data is used to build profiles of people and goods with an assumed security risk and take (preventive) actions on undesired situations.

These developments enable a shift from reactive security authorities, after the fact collecting of information and evidence, towards proactive security enforcement, using technology to anticipate on and prevent crime. Note that we already experience a tendency towards prevention, also in legislation, that is supported by technology developments but not dependent on it. In this sense the technology is enabling as well. Except for being enablers, converging technologies may also be a driver for new 'paradigms' in the security application field. We sketched a more participatory role of citizens in forensic research (lab in your pocket) or social crime control (prison without walls) as examples.

The impact of converging technologies on security applications, however, is dependent on two uncertainties we identified, namely the degree up to which the processing capacity keeps pace with the growing amount of information and the readiness of actors to share their information.

Note that in our scenarios, we observe a dominant role of information technology. This is not because ICT developments have a larger impact that nano, bio or cognitive developments; neither do we want to stress ICT as the glue between all technology developments. The main reason is because of our application area, i.e., the three cases of monitoring and immediate action, forensic research and profiling and identification. For example, except for DNA and lab-on-a-chip applications, biotechnology plays a less dominant role in these cases, at least for the coming 15 years. Moreover, the practical applicability of nano and cognitive technologies is a matter of the long term anyhow. For the same reason, our impact analysis has an emphasis on the relationship between

government and citizens, more that the mutual relationship between citizens. Applying the technology developments in other cases will result in different emphasises.

We started with the technology developments, wrote scenarios based on these developments, and then analysed the normative and social impacts of these scenarios. Eight trends have been distinguished:

1 Shifts in data collection and data processing: More and more data are being created; they are disseminated more widely, to a larger number of parties; access to data is made easier for the government, and control over these data is becoming increasingly difficult for data subjects. The consequence of this trend is that, even with the same investigative powers, governmental authorities are in a position to collect and use significantly more data about citizens than before, and this increase is not only quantitative but also qualitative. This in turn enables the government, in principle, to know better than ever before what citizens, including criminals and terrorists, are doing.

2 Shifts in methods of surveillance: Increasing possibilities of surveillance will induce more normalising effects on conduct, self-perception, personality, and world-view, than ever before.

3 Shifts in power relations: Regulation will be delegated more from persons to technology and from public, governmental parties to private organizations and citizens.

4 Changes in the governability of technologies themselves: Growing uncertainty and complexity will increasingly complicate the governance of the emerging technologies and their applications.

5 Shifts in privacy concerns: As new possibilities of observation and surveillance show both centralizing and decentralizing tendencies (that do not mutually neutralize each other) and instruments for observation and surveillance become increasingly unobtrusive, both the perception and nature of privacy invasions will change.

6 Shifts in the focus of criminal law, away from prevention, retribution and rehabilitation, towards risk prevention.

7 Shifts in the conceptions of freedom and personal responsibility may affect the ways in which persons perceive their own and others' identities; they need not automatically undermine conceptions of morality and law that take personal responsibility and free will as their starting points.

8 Increasing fusion of norms and their enforcement, and in its wake: challenges to certain moral outlooks and new questions regarding the legitimacy of new regulatory and enforcement arrangements.

During a period of 15 years, however, the prevailing standards and trends in society evolve as well. Examples of this co-evolution are, e.g., health risk of nano-particles of chip implants that have a restraining influence on the technology developments (due to less investments, public opinion or governmental rules). Because of our research questions and method chosen, however, the scenarios have been driven by technology developments. Therefore, some developments in the scenarios may be controversial. However, that exactly is the purpose of scenarios (to elicit discussion), they way we used them (impact analysis) and the way they may be further used to start debates, either

internally (the role on Ministries, the impact of their policy on scenarios) or externally (social debate). In this way the technology forecasts, scenarios and impact analysis may be used to give shape to new policies, which in turn will possibly influence the technology developments.

11 Addendum: The trends and the normative framework of the Dutch criminal law

We concluded Chapter 9 with a note on the co-evolution of technology and the normative outlook. Because of this co-evolution, an evaluation of the scenarios on the basis of the trends that we sketched in that chapter should only be undertaken with due reservation. It may, nonetheless, be interesting to confront the trends with the current Dutch normative framework for criminal law, particularly its underlying principles. This can highlight possible frictions and occasions for choices. In this additional chapter, we present the starting points for such a thought experiment.

Law enforcement is an important function within democratic constitutional states. It embodies the state monopoly on the use of force in order to guarantee and maintain law and order. Given the significant effect that law enforcement, and especially punishment, can have on individuals, it is essential to maintain strict boundaries on the operation of law enforcement and the judiciary. A balance has to be struck between the interests of society and those of the individual.

The boundaries within which law enforcement has to operate consist of a complex framework of concrete legal provisions, such as the Code of Criminal Procedure (*Wetboek van Strafvordering*) and the Criminal Code (*Wetboek van Strafrecht*), and a large body of case-law. But also, more abstract principles as formulated in the Constitution and international treaties to which the Netherlands is a signatory shape the landscape in which actions have to be assessed. And finally, there are (even more abstract) unwritten principles that provide the foundation for our democratic constitutional state. These abstract principles have a two-fold role. On the one hand they provide guidance with respect to the interpretation of concrete statutory provisions. For instance, the freedom of speech purports to protect a public debate. This principle can help to determine whether a specific expression in the media should be considered defamatory. The second function of principles is to guide what is to be regulated in society and how. Adhering to the presumption of innocence in criminal law implies that certain safeguards have to be defined in the criminal procedure, such as a right to remain silent, and a burden of proof on the government's side to prove an accusation.

Eliciting the principles that lie at the heart of the Dutch constitutional state can help to assess the boundaries of the adoption of converging technologies for the purposes of monitoring people, improving forensic techniques, and profiling, identifying and monitoring potentially dangerous individuals or groups. These principles are not set in stone for eternity, however. They are co-evolving with the social and technical developments and with the changes in the relation between the interests of society at large and those of the individual. The inventory of principles and current (fundamental) rights merely clarifies where choices and trade-offs could be made.

To ease readability, we divide the framework in three: principles of the democratic constitutional order, constitutional rights, and principles of criminal law. For each section, we outline the normative principles first, and then we address a number of possible tensions arising as a result of the technical developments and the social and normative trends sketched in the previous chapters and sections.

11.1 The normative framework

11.1.1 The democratic constitutional state

The democratic constitutional state (we base ourselves here largely on Gutwirth and De Hert, 2005) is a specific concept of state in which the exercise of power is, by definition, limited. This limitation of power is embodied in three fundamental principles, namely the recognition of fundamental rights and liberties, the rule of law (constitutionalism), and democracy.

Firstly, the constitutions of democratic constitutional states contain a set of individual fundamental rights and freedoms (or shortly: human rights) which are deemed to be at the very core of the political construct. In principle, the State is not allowed to encroach upon or to interfere with these rights. Human rights express the recognition of the power of the individual, drawing the limits and frontiers of the power of the state and of state intervention. This function of human rights covers what Berlin termed 'negative freedom': freedom from interference[49]. In addition, human rights and liberties have a political function because they empower citizens (or individuals) to participate in the political system. Here we find basic liberties, such as freedom of expression, liberty of conscience and freedom of association, that enable citizens to develop and exercise their moral powers in forming, revising and in rationally pursuing their conceptions of the good.

Secondly, the constitutions of democratic states enshrine the rule of law and constitute a constitutional state. The rule of law again limits the power of government, but not through setting a limit to the reach of the power (as is the case with human rights), but through the organisation of government and power. The objective remains the same, namely the protection of individuals against excessive and arbitrary domination. The main idea of the rule of law is the subjection of government and other state powers to a set of restricting constitutional rules and mechanisms.

First, the rule of law provides for the principle of legality of government; power can only be exercised in accordance to the law. From this perspective, public authorities, especially including law enforcement, are bound by their own rules and can only exercise their powers in a lawful way. All powers must derive from the constitution (which in its turn is deemed to translate the will of the sovereign people) and any exercise of power must derive from a constitutional provision. This implies that government is accountable and that its actions must be controllable, and thus transparent. 'The rule of law' thus refers to the idea that our societies are governed by rational and impersonal laws and not by the arbitrary commands of humans. Moreover, because these laws must be general and apply to all, they (at least formally) embody the principle of equal treatment and protection of the laws.

Second, the rule of law establishes the trias politica or, in other words, a system of checks and balances of powers. The power of the state is distributed over different institutions, with different competencies and functions. These powers - the executive, legislative and judicial power - are constitutionally doomed to work together through a dynamic system of mutual control or checks and balances. Such a system implies the

[49] Cf. F. Kuitenbrouwer. Het recht om met rust gelaten te worden, Balans, Utrecht 1991.

mutual accountability of state powers, and hence the reciprocal transparency and controllability of the legislative, the judicial and, last but not least, the executive power.

Within the field of law enforcement, this kind of balancing of power is evident in the requirement of judicial oversight of actions that infringe upon the individual's fundamental rights, such as the inviolability of the home. Searching homes and wiretapping can only take place with the approval of a neutral third party, such as a court.

Third, the constitutions of democratic constitutional states recognise the postulate of the people's sovereignty and the principles of democracy and democratic representation. The only valid justification of power must be sought in the citizens' consent or will and state power therefore is derived from the sovereignty of the citizens. 'Democracy' entails that government is driven by the public or general interest and must take into account the will of the majority. Hence, systems of representation and participation of citizens are of crucial importance. Constitutional bodies and institutions must be representative. Participation of citizens in political decision-making must be organised and stimulated. And, last but not least, systems of democratic governance must foresee procedures of direct and indirect control of the public authorities by the citizens. As a result democratic rule implies the accountability of the government towards the citizens, which again calls for transparency of public decision-making and policies.

With respect to the use of converging technologies in law enforcement, the principles of the democratic constitutional state require democratic support and that its use has to be regulated by law. This is especially so when adoption of these new technologies is likely to affect the fundamental rights and liberties.

Fourth, important to bear in mind is that the Dutch legal order is, to a considerable extent, part of a wider, supranational, order. Despite the fact that the concept of the democratic constitutional state relies on sovereignty of the Dutch people, the Dutch legal system is thus also affected by foreign elements. The Netherlands are signatory to a number of international treaties that address fundamental human rights, such as the European Convention on Human Rights (1950) and the UN International Covenant on Civil and Political Rights (1966). These treaties have a (limited) direct effect and open a road for individuals to present cases involving breaches of rights and liberties granted in these treaties before international courts, such as the European Court of Human Rights. Also, Dutch courts will generally rule in accordance with case-law of these international courts. The rights and liberties expressed in these international treaties are therefore to be taken as part of the Dutch legal order. This means that the Netherlands can not move aside certain fundamental rights without reconsidering its position with respect to these treaties.

A similar situation exists as a result of the Dutch membership of the European Union. Especially with respect to technological developments legislation has to be drafted or amended as a result of obligations created by regulations and directives (first pillar) or by decisions and framework decisions (third pillar). Also, the Council of Europe's Convention on Cybercrime clearly affects the Dutch legal order. The Netherlands take an active role in the development of these international instruments, but the final outcome is a compromise which may not completely satisfy Dutch interests or policies. This means that principles at the level of the EU and the Council of Europe limit the headroom for the Dutch legislature to act sovereignly. It also means that conflicts may arise when EU regulation limits rights and liberties granted in the Dutch Constitution.

11.1.2 Constitutional rights

An essential safeguard in the government-citizen relationship is constitutional rights. Constitutional values are important for technology policy and law, but in an indirect way: they often play an implicit role, through legislation that embeds and implements constitutional rights. In shaping the law and legal policy to face future, technology- and surveillance-related developments, constitutional values can therefore serve as an important guide to lead society through radical changes, particularly since it is hard to foresee in a timely manner which changes exactly are brought about by new technologies (Leenes and Koops, 2007).

With respect to converging technologies in law enforcement, a number of fundamental rights are at stake:

- non-discrimination: Article 1 of the Dutch Constitution states that all persons in the Netherlands shall be treated equally in equal circumstances. Discrimination on any ground shall not be permitted. This principle implies, for example, that if limits are imposed on the freedoms and liberties of certain individuals this has to be justified and warranted by law. A specific corollary of this is the principle of:
    - probable cause: Article 27 DCCP provides a ground for treating certain individuals – suspects – differently from other individuals. An important condition for being treated as a suspect is that there have to be reasonable grounds, based on facts and circumstances, for law-enforcement activities against an individual suspected of having committed a crime;

- freedom of expression: the freedom of expression (Art. 7 Dutch Constitution) is a principle deeply embedded in Dutch society. A certain liberty of the press has always prevailed in the Netherlands: as early as the 16th century, no prior censorship was applied. Freedom of expression is an important fundamental right that limits state power, but maybe more importantly, it is necessary, as a political right, in a democratic society. Citizens need to be able to express themselves freely in order to facilitate public debates and the forming of public opinion, which in turn contributes to democratic decision making;

- the right to respect for private life or privacy: this right is the core of Art. 8 ECHR and Art. 10 para. 1 DC. It refers to a special interest individuals have in being able to be free from certain kinds of intrusions. The reasons for desiring this kind of privacy are diverse, but often relate to the fact that respect for private life is important to safeguard personal liberties and autonomy (Vedder, 2004; Vedder and Blok, 2005). Apart from intimate life as the core of Art. 10 para. 1 DC (Blok, 2002: 58-59), the right to respect for private life also includes elements that have separate provisions in the Dutch constitutional order:
    - data protection: closely related to privacy, although carrying distinct elements of its own, the right to data protection is embedded in Art. 8 ECHR and Art. 10 paras. 2-3 DC. The constitutional provision only explicitly mentions information and correction rights, but other data-protection principles as laid down in international instruments (such as Directive 95/46/EC), including purpose-specification, data minimisation, and adequate supervision, are equally valid in the

Netherlands (cf. the Dutch Data Protection Act). However, data protection is limited to individual natural persons: group profiling falls outside the scope of data protection (cf. Vedder, 1998; Custers, 2004);

- the inviolability of the home: at least since 1798, the inviolability of the home has been a fundamental right for the Batavian people; Art. 12 DC protects citizens against entry into their home without their will, barring exceptions laid down in or pursuant to law; in light of NBIC, the term 'entry' (*binnentreden*) is relevant, since it involves physical entry and hence does not as such cover monitoring a home from the outside (Koops and Groothuis, 2007);

- the inviolability of the body: Art. 11 DC stipulates that everyone has the right to inviolability of his body, without prejudice to restrictions laid down by or pursuant to law. This entails a right to resist acts aimed at infringing the integrity of one's body; it covers integrity of the mind, but only to the extent that the body is physically affected in the act (Koops and Groothuis, 2007);

- the secrecy of communications: Art. 13 DC contains the right to secrecy of letters (paragraph 1 – only to be infringed by order of a judge) and secrecy of telephone and telegraph (paragraph 2 – to be infringed by those designated by law). Although this provision is badly in need of updating, it is nowadays generally accepted that email should have the same constitutional protection as telephone conversations (and criminal law provides similar protection against government intrusion), and that infringements require authorisation from a judge (or in cases of national security: a minister) (Koops and Groothuis, 2007);

- the right to a fair trial: Art. 6 ECHR ensures the right to a fair trial, which includes many elements; relevant for our purposes are at least the following elements (see Harteveld, Keulen and Krabbe (1996) for an overview):

  - a hearing by an independent and impartial tribunal;

  - within a reasonable time (likewise, Art. 15 para. 3 DC);

  - being presumed innocent until proved guilty;

  - privilege against self-incrimination;

- the right to liberty and security: Art. 15 DC and Art. 5 ECHR stipulate that nobody shall be deprived of their liberty. Exceptions are allowed for a number of purposes, including conviction, and pre-trial detention for the purpose of bringing him before a court on reasonable suspicion of having committed an offence, or when it is reasonably considered necessary to prevent his committing an offence or fleeing after having done so. This right also includes specific elements (see Harteveld, Keulen and Krabbe (1996) for an overview):

  - the right to be brought promptly before a judge;

- the right to challenge the lawfulness of deprivation of liberty.

11.1.3 Basic principles of criminal law

The normative framework to assess NBIC and CT applications for crime-control purposes should not only include constitutional rights and principles of the democratic constitutional order, but also basis principles of criminal law. We mention here those principles valid in the Dutch legal order that have relevance for the purposes of this study.

One of the most general principles of criminal law is that it is a last resort (Van Hamel 1880: 12-13; Smidt 1881: 11). As Justice Minister Modderman phrased it on 25 October 1880 at the introduction of the current Dutch Criminal Code: 'The principle is this: first, that only that may be punished, which is *injustice*. (…) Second, the requirement is added that this is an injustice of which experience has shown that (of course, taking the current societal context into account) it cannot properly be controlled by any other means. The threat of punishment must remain an *ultimum remedium*' (Smidt 1881: 11, our translation). This means, among other things, that activities should, in principle, only be criminalised if they are harmful and if there are no effective and efficient other ways of combating this harm. Numerous exceptions exist nowadays to this rule – criminalisation is, for example, quite often used as an instrument of administrative control – but the general rule remains valid today.

Relevant principles of substantive criminal law (Remmelink, 1995: 70-72) include:

- the substantive legality principle embodied in Art. 1 CC: *nulla poena sine lege previa* (no punishment without a prior law). A consequence of this principle is that only those penalties that had already been established for the offence at the time when it was committed can be imposed;

- the *lex certa* principle: criminalisations must be clearly and strictly formulated, so that citizens know which behaviour they should avoid if they do not want to get punished;

- no punishment is given without guilt: if someone cannot be blamed for harmful behaviour, he must not be punished for this. This principle is closely related to the notion of free will, from the assumption that people can only be blamed for acts they have a choice to do or not do (cf. supra, subsections 9.1.1 and 9.1.2).

In procedural criminal law, there are various other relevant principles (Corstens, 1995: 49-69). Besides those principles that function as constitutional rights (right to a fair trial, right to freedom, see above), these principles include:

- proportionality and subsidiarity: law enforcement activities may infringe constitutional rights only to the extent that they are proportionate to the crime under investigation and when there are no less infringing measures available;

- procedural legality: all investigation powers must be described clearly and strictly in law (Art. 1 DCCP);

- expediency principle (*opportuniteitsbeginsel*): the Public Prosecutor has a discretionary power to decide whether or not to prosecute a particular crime;

– equality principle: similar cases must be treated similarly (cf. Art. 1 Dutch Constitution: discrimination on any ground is forbidden); this is closely related to the principle of no arbitrariness: law enforcement must be consistently applied;

– immediacy principle: evidence is presented and assessed in court during a criminal trial;

– material truth: the judge in a criminal court seeks the 'real' truth rather than some form of procedural truth, and he can convict only when internally convinced that the suspect is guilty;

– integrity of purpose: investigation powers may not be applied for other purposes than for which the power has been created (a prohibition of *détournement de pouvoir*).

11.2 Applying the normative framework to the trends

11.2.1 The democratic constitutional state

The changing nature of law

The shift of law becoming more morally-neutral by the inclusion of forced compliance mechanisms in technology (*supra*, 9.1.2 trend 2) has several consequences for the nature of law.

First, the element of choice that is inherent to our current legal system is important not only from the perspective of the assumption of the free will, but also because it enables civil disobedience. If we grant that laws are not always just by definition (i.e., by the mere fact that they are a law) – and there are sufficient examples in history to warrant this assumption –, there is always a possibility that a law is – in general or when applied in concrete cases – unjust. Civil disobedience is an important mechanism to correct such unjust laws or applications of laws.

Building in enforced compliance therefore entails the risk of backfiring when the norms built-in are somehow unjust. For example, the knee lock in scenario B seems straightforward enough: it prevents a convict or person detained at Her Majesty's pleasure from running away to escape. At the same time, however, it may also prevent him from running away in order to save a person who is just about to drown in a canal further on and who is urgently crying for help, and it might prevent him from running away in order to escape a balcony falling down from a building. Of course, such things will not often occur, but the fact of making (civil) disobedience technically impossible lays a heavy burden on the built-in norm to be correct and to be always applied correctly. For knee locks, this means for example that they should not be triggered completely automatically, but always after human intervention, e.g., by an accompanying or video-surveilling officer, at least until technology becomes sophisticated enough to estimate situational contexts in the same degree of precision as humans do (which will take much longer than 15 years).

Second, enforcing norms through technology, and thus taking away the choice not to comply, also has repercussions for the image of human nature as mirrored in law. Law with built-in compliance tends to relate to a deterministic and completely functional view of the world and mankind. To put it boldly, as the moral element dissolves from legal norms and their application, man is reduced to a mechanistic instrument without an

autonomous will, intelligence, or conscience. Of course, using more technology to enforce compliance with legal norms does not immediately reduce citizens to will-less instruments, but it does, in small steps, reduce human autonomy. According to Roger Brownsword, technology should not be allowed to create 'perfect' compliance with 'perfect' rules, since humanity is thereby reduced to flatness. Some kind of flawedness or fallibility needs to exist in order to enable people to experience being human, and hence, allowing choice is essential when 'techno-regulation' supplements or supplants the prescription of norms in law (Brownsword, 2004: 230-232).

Involving non-state actors in law enforcement

As was already pointed out in subsection 9.1.3, as a result of the technological developments, newly emerging polycentric governance and regulatory regimes will persist and become gradually more important. Responsibilities for law enforcement, hitherto resting with national state authorities, will gradually extend to other organisations, such as supra- and international organisations and (alliances of) business corporations and even NGOs. From the vantage point of the ideals of the democratic state and the rule of law, this is in principle not an attractive prospect. The system of law enforcement will become more complicated, and possibilities of democratic control will diminish accordingly. It is therefore desirable that the legitimacy of private and supranational organisations is safeguarded if they are enlisted to perform law-enforcement functions. Guaranteeing transparency, adherence to constitutional rights, and some sort of supervision by democratically legitimised government and parliament or other forms of legitimisation could counterbalance the potential deficit in democratic legitimacy.

The citizen-government relationship

What are the implications of the converging technologies applications and the trends sketched in this report for the citizen-government relationship? A first conclusion is that the balance of power is shifting. The technology- and security-related extension of investigation powers, reinforced by the quantitative and qualitative increase in data, has been primarily viewed by the legislature from the perspective of fighting serious crime – a battle of arms between police and criminals with technology as a primary instrument. What is often overlooked, however, is the net effect of this battle of arms on the average, innocent citizen, who is now under increasing surveillance without probable cause. Through the cumulative effect of diverse parts of surveillance, citizens are becoming more transparent to the government, and citizens risk being in a weaker position than before if the government uses its increased power of knowledge in making decisions about them. As the obtrusiveness of surveillance gradually diminishes (think of RFID tags) citizens will have more difficulty with discovering that the authorities are in the possession of information about them and with what kind of information they possess. Consequently, their position to defend themselves is weakened, even when decisions, suspicions or accusations on the basis of that information are wrong.

The shift in balance of power between government and citizens impacts the liberty and security of citizens. The scenarios imply a move towards a culture of control and criminal law as a first resort, carrying with it increasing distrust: people may tend to *a priori* distrust strangers and unknown situations, and trust may therefore be decreasing as a primary basis in societal relations. It needs to be carefully researched what the longer-term effect is of such a trend on citizens' freedom. Conceivably, an attitude of distrust and the knowledge of being under constant surveillance has a chilling effect on citizens'

freedom to develop themselves (fostering their identity) and to act uninhibitedly (fostering their privacy and autonomy).

An increased government power of knowledge over citizens is not necessarily wrong, since changes in society may warrant such a shift. However, it should be carefully argued that increased surveillance is indeed necessary, and empirical data are required to substantiate this. Steps towards preventative crime control have often been taken up to the present in a rather matter-of-fact way; the whole process is piecemeal with small individual steps, which together may constitute a giant leap (cf. Vedder *et al.*, 2007: 66-68 on the cumulative effect of measures). The policy and societal debates often focus on the individual steps rather than on the entire leap, and it is questionable whether a cumulative move towards surveillance is evidence-based and well-considered. A key recommendation for legislatures is to pay more attention to empirical underpinning of surveillance measures and their cumulative effect, to commission evaluation studies, and to use sunset clauses in legislation in case a measure does not show effect.

Also, more checks and balances are required. The increased government power needs to be balanced by additional checks, notably with more transparency requirements (citizens must know which data are being collected and processed for which purposes) and with enhanced audit and supervision. Independent authorities should regularly check whether the government uses its powers correctly and legitimately; the criminal court is no longer the primary instrument to check the execution of investigation powers, since many cases are not brought before the court, and alternative supervision mechanisms should be considered. Why this is important, is succinctly expressed by attorney Thomas Connolly, who said: 'It is about the enormous power government officials have. (…) Whatever the government can legally do to Steven Hatfill, it can legally do to any of us' (*USA Today* 27 August 2003). Steven Hatfill was accused of having spread anthrax, although he had nothing to do with it, because the police wanted to have the public believe that progress was being made. Such cases of abuse of power only come to light when well-functioning audit and supervision mechanisms are in place.

Likewise, more information security is needed, since the police, in massive data collection, easily risks using incorrect or outdated data (see, e.g., *Keegan* v. *UK*, ECtHR 18 July 2006). When data mining and profiling are used for criminal investigation and intelligence, mechanisms need to be in place to ensure careful application of profiles to individuals; citizens should not be confronted with government investigation merely because they fit a suspect profile.

11.2.2 Constitutional rights

An in-depth analysis of constitutional rights in light of the trends highlighted in the previous chapter is not possible in the scope of this report. We restrict ourselves here to giving some examples of relevant issues:

- non-discrimination, probable cause: Placing (certain) people under permanent surveillance without a clear cause, for instance by embedding RFID tags or other MEMS, may conflict with the non-discrimination principle.

- identity/anonymity: Although the Dutch interpretation of freedom of expression does not include an explicit right to anonymous expression of thoughts and opinions, anonymity is important to the freedom of expression. The reason is well-formulated by the US Supreme Court, in their interpretation of the First Amendment right to free

speech: '[T]he interest in having anonymous works enter the marketplace of ideas unquestionably outweighs any public interest in requiring disclosure as a condition of entry. Accordingly, an author's decision to remain anonymous (...) is an aspect of the freedom of speech protected by the First Amendment' (*McIntyre* v. *Ohio Elections Commission*, 514 U.S. 334, 342, 1995). Tagging individuals, monitoring, and profiling are activities that as a side-effect may have a chilling effect on the freedom of expression, because they in effect result in identifying individuals. Attributing expressions to specific individuals then becomes easier, so that some people might feel inhibited to utter their thoughts and opinions freely, for example, on the Internet.

– bodily integrity: This covers integrity of the mind, but only to the extent that the body is physically affected in the act (Koops and Groothuis, 2007); this implies for converging technologies that neuro-stimulation from the outside, and certainly from within by means of neuro medication affects not only the individual's autonomy and free will, but also his bodily integrity.

These examples show that a critical assessment of the developments in NBIC and converging technologies in relation to constitutional rights and other fundamental anchor points of society is required. Such an assessment could lead to a reconsideration of existing or proposed future measures, the establishment of substantial new types of checks and balances to counter-balance the shifts in societal and government-citizen relationships outlined above. However, they could also lead to a reconsideration of the normative framework, some elements of which might be judged to need a re-interpretation in light of converging technologies.

11.2.3 Basic principles of criminal law

The shift towards prevention (*supra*, trend 6) moves away from the traditional role of criminal law as reactive and an *ultimum remedium*. This has several consequences that should be taken into account.

1 The notion of punishment should be reconsidered. The customary types of intervention will change as will the reasons for intervention. The technological developments are likely to elicit a tendency away from retribution on the basis of guilt towards influencing and improving behaviour. This affects, for example, the right to a fair trial (Art. 6 ECHR), which in the interpretation of the Court applies to government interventions with a 'punitive' element. Perhaps the scope of Art. 6 ECHR should be re-interpreted if there is a significant move from reactive to preventive interventions for law-enforcement purposes.

2 Along the same lines, the whole system of checks and balances may need to be reinvented because of the trend towards prevention. The current criminal-law system very much centres on judicial supervision – investigating judges supervising the most infringing investigation measures, and the judges in court supervising the fairness of criminal procedure in general. One challenge is therefore to ensure a similar level of safeguards when in a policy of preventative measures no judges enter the picture, because there is no crime under investigation. This challenge cannot simply be met by transplanting checks and balances from criminal law to, for example, administrative law, because the preventative measures will not always be taken by administrative bodies, but by a plethora of public and private actors. Establishing new checks and balances will require a lot of effort, creativity, and commitment from all relevant parties.

3 A far-reaching consequence of converging technologies applied in early-warning systems might also be that people are triggered into behaving in certain ways. For instance, RFIDs and other sophisticated identification technologies may prevent people from being anonymous. When people are aware of being watched or monitored continuously, disciplining effects may arise: they may act differently than they would otherwise have done. In the previous chapter we already gave the example of the speed cameras. In particular, treating an individual on the basis of certain (group) characteristics may reinforce that characteristic as a part of the individual's sense of identity: society then stigmatises individuals into behavioural patterns (cf. Goffman, 1963). In this way, predictive behavioural models may have self-fulfilling prophecy effects. For instance, people who are expected to show criminal or aggressive behaviour may be treated accordingly, without having done anything yet, and this in turn may trigger them into behaving in the 'expected' way.

4 The equality principle holds that equal cases are to be treated equally. A result of the trends described is that much more data related to individuals are being collected and ascribed to these individuals. The resulting profiles provide rich data sources with respect to these individuals from which, arbitrary, features can be extracted that differentiate a particular individual from others. Hence, these fine-grained data sources can be used to argue that a certain individual should not be treated like others.

Also with respect to products and services, equality may lose ground because identification facilitates personalisation. Individuals may therefore increasingly be treated as individuals rather than as part of a group (e.g., teenagers, women, students, repeat offenders). And because they are individualised, they may also be increasingly be held accountable for their own behaviour. The debates about giving up the solidarity principle as one of the leading principles in (health) insurances and charging and treating unhealthy people (e.g., smokers, obese) differently fits this trend.

5 The immediacy principle tries to preserve the integrity of a judgment by ensuring that arguments and evidence are put to the judge in the most direct manner possible. This means that proof ideally has to be presented to court by those who collect and interpret the evidence and that testimony is presented before the court as well (related to the orality principle). This principle is under pressure when the legal system shifts from retribution to prevention. In the pre-crime scenario, interventions take place before the harm has been inflicted. How is the court to judge on these interventions if the necessary proof and arguments to condemn the purported criminal behaviour are absent because of the intervention?

6 In a strict sense, pre-crime interventions prevent crimes from taking place and hence, if there is no crime, there is no crime to be judged and therefore no necessity for a trial in the traditional sense. The shift from retribution to prevention implies that legal provisions criminalising behaviour may have to be amended. The focus could move to preparatory aspects of the crimes, instead of on the crimes themselves. The effect of the pre-crime interventions is partly to prevent criminal behaviour (e.g., interventions by means of drug induced behavioural corrections), in which case there will not be any trial, and partly to stop criminals before they commit their crimes. The latter case is basically a kind of preparatory act or criminal attempt. However, the trends predict that the period between having sufficient information to intervene and the criminal acts to be prevented will grow. So, instead of catching a burglar at the brink of inserting a crowbar in a window pane, future interventions may even occur when this individual considers buying a crowbar, for instance. This will also have a bearing on the trials that do take place. The

longer the period between an intervention and a purported/predicted criminal activity, the more possible worlds (choices) there are and the more likely alternative interpretations of actions can be given. This means that providing evidence of criminal intent will become even harder than it is nowadays in the case of preparatory acts and criminal attempt.

7 Providing evidence in itself will become increasingly complex because it will largely be based on technical proof. This has two effects. On the one hand the role of expert witnesses will become more important. Experts will have to provide arguments for the validity of proof and its interpretation. At present, the role of experts in criminal trials is not clearly regulated in the Netherlands. Another issue is the strong role the Netherlands Forensic Institute plays in this respect. The dependency on just a single source of technical expertise and forensics creates risks with respect to checks and balances. There will be a growing need for second opinion labs and forensic competition. The quality of forensics labs will have to be assessed and clear procedures for selecting a concrete lab for a specific trial will have to be developed.

Reliance on technical evidence also presents problems in the judiciary. Numerous studies have shown that people have difficulties in understanding complex statistical evidence, and judges are no exception here. More complex technical proof will require more expertise amongst the judiciary to assess this kind of proof. Training of the judiciary is important, but judges cannot become technical experts; their task is to establish the legal consequences of certain acts. To overcome risks of arbitrary assessments of technical proof, standards for technical evidence may need to be developed.

8 There are also issues concerning identity and identification. One side-effect of increasingly sophisticated and pervasive identification techniques is that it might change and even exacerbate criminal behaviour in certain cases. For example, several criminals intentionally spread other people's hairs at a crime scene in order to complicate the investigation; some are even purported to collect hairs already when in prison for use in future crimes (making sure that there will be hits in the DNA database). When a bank robber knows he has been spotted recognisably on cameras in the street and in the bank, he might resort to more violence in order to escape quickly. When DNA fingerprinting became more widely used in the 1990s, some rapists committed extreme violence (including mutilation) in order to try to remove sperm traces. These effects are, of course, not a reason to refrain from more sophisticated identification techniques, but some of these mechanisms are foreseeable and should be taken into account when introducing new measures in order to prevent or minimise these harmful side-effects.

Besides, policy makers should also realise that changes in identification measures also have long-term effects on criminal evidence. DNA fingerprinting has led to strong evidence, but as crime-scene technology becomes more sophisticated, the number of traces will multiply. For example, when in scenario C traces of 25,000 people are found, even if most can be eliminated straight away, still some 200 people are left to investigate further. This is useful as a lead in investigation, but the fact of a DNA trace being found at a crime-scene will be much less substantial evidence in court when 200 potentially relevant people have such traces. Again, this is no reason to refrain from using innovative identification techniques, but policy makers should be aware of long-term effects of these techniques, so that they can timely anticipate shifts in criminal procedure and evidential value.

Samenvatting (in Dutch)

Deze studie over *convergerende technologieën* kijkt 15 jaar vooruit en is bedoeld voor uitvoerders en beleidsmakers op het domein van de maatschappelijke veiligheid. We nemen in deze studie de technologieontwikkelingen als uitgangspunt. We onderscheiden vier convergerende technologieën: nanotechnologie, biotechnologie, informatietechnologie en cognitietechnologie (afgekort NBIC technologieën). We schatten in wat de ontwikkelingen zullen zijn, vertalen deze ontwikkelingen naar het toepassingsdomein, en doen een analyse van de ethische, wetgevende en sociaal maatschappelijke impact van deze toepassingen. We maken daarbij gebruik van drie casussen om de toepassing van convergerende technologieën af te bakenen. Deze casussen betreffen het monitoren en volgen van voorwerpen en personen en het op afstand ingrijpen bij ongewenste bewegingen; het verbeteren en ontwikkelen van forensisch sporenonderzoek; en het profileren, identificeren en monitoren van personen met een al dan niet verondersteld veiligheidsrisico.

In onze aanpak zijn we gestart met de technologieontwikkelingen (los van de toepassingen), hebben we toepassingsscenario's geschreven puur op basis van de technologieverwachtingen (los van de impactanalyse), en is ten slotte de ethische, juridische en sociaal maatschappelijk impact van deze scenario's geanalyseerd, resulterend in een opsomming van acht trends. De resultaten van dit onderzoek kunnen worden gebruikt voor zowel het interne debat (de rol van de betrokken ministeries, de impact van hun beleid op de scenario's) als een maatschappelijk debat. Op deze wijze kunnen technologieverkenning, scenario's en impact analyse bijdragen aan nieuw beleid, dat op zijn beurt de technologieontwikkelingen mogelijk weer beïnvloedt.

Dit rapport bestaat uit drie delen. Het eerste deel beschrijft de stand van zaken rond de vier genoemde technologieën, de hier te verwachten toekomstige ontwikkelingen, en de ontwikkelingen op het gebied van de convergentie tussen deze technologieën. Het tweede deel beschrijft de (toekomstige) toepasbaarheid van de convergerende technologieën in het applicatiedomein, in het bijzonder de drie genoemde casussen. Dit deel eindigt met een viertal scenario's. Deze illustreren de technologieontwikkelingen via toepassingen en worden gebuikt als basis voor de impactanalyse van de technologieontwikkelingen. In het derde deel worden deze scenario's geanalyseerd op hun ethische, wetgevende en sociaal maatschappelijke aspecten. Dit deel beschrijft de belangrijkste sociale en normatieve trends die we waarnemen.

Nanotechnologie

Nanotechnologie is een algemene term die de technologieën omvat die werken met eenheden, materialen en systemen waarvan tenminste een van de relevante afmetingen in het schaalbereik van 1 tot 100 nanometer ligt. Een kernaspect is daarbij dat specifieke (nano)eigenschappen een rol spelen, zoals het beïnvloeden van eigenschappen van grote oppervlakken of kwantumeffecten. In het algemeen worden voor de nanotechnologie drie deelgebieden onderscheiden:

– Materialen en oppervlakken, of de eigenschappen daarvan, die gefabriceerd worden met nanotechnologie. Deze nanomaterialen vormen inmiddels een volwassen technologiegebied dat is doorgedrongen in veel producten in de handel zoals cosmetica, verf en andere oppervlaktebehandelingen, weefstoffen, lijm- en kleefstoffen, katalysatoren en materialen met verbeterde eigenschappen.
– Micro/nano-elektronica. Nano-elektronica laat een mengeling zien van steeds doorgaande verbeteringen en nu al bereikte prestaties zoals de hoge capaciteit van schijven en chips in MP3/4 spelers, geheugensticks, en computers. Daarnaast leidt de nano-elektronica ook tot productieverbeteringen in de gangbare elektronica met steeds meer schakelingen op een chip van steeds kleinere afmetingen. De doorgroeimogelijkheden zijn hier enorm.
– Bionanotechnologie en nanogeneeskunde. Met behulp van DNA microchips is het tegenwoordig mogelijk om de activiteit van tienduizenden genen tegelijk te bemeten en bepalingen die voorheen alleen in een laboratorium konden worden uitgevoerd passen nu op een chip waarbij minieme hoeveelheden monstermateriaal volstaan. De ontwikkelingsmogelijkheden van deze lab-on-a-chip zijn nog lang niet zijn uitgeput. Een andere toepassing van bionanotechnologie vinden we in de sensoren en actuatoren. Biosensoren kunnen op locatie concentraties en stoffen detecteren waardoor het nemen van monsters voor laboratoriumanalyse (de zogenaamde ‘point of care’ analyse) minder noodzakelijk wordt. De actuatoren (zoals minuscule pompjes, motoren, e.d.) kunnen heel precies medicijnen toedienen wanneer een sensor bijvoorbeeld een verstoring van een evenwicht detecteert.

Een belangrijke poging om een alomvattend toekomstbeeld voor de nanotechnologie te schetsen is Mihail Roco’s viergeneratie model. Roco is senior adviseur van het Nationaal Nanotechnologie Initiatief in de Verenigde Staten. Volgens Roco’s model bestaat de eerste generatie nanotechnologie uit reactieve ‘slimme’ materialen en structuren die in staat zijn om hun eigenschappen te veranderen als antwoord op de veranderde externe omstandigheden (zoals temperatuur, elektromagnetisch velden, vochtigheid, enzovoort). Deze slimme materialen combineren dus de eigenschap om waar te nemen met die om daarop met een verandering van eigenschap te reageren. De volgende stap in Roco’s model is om in deze nanomaterialen een vorm van informatieverwerking te integreren zodat actieve keuzes kunnen worden gemaakt en naar keuze kan worden gehandeld. Nanotechnologie zal het mogelijk maken om zulke functies verder te verbeteren en te veranderen. Verder gaande convergentie van technologieën leidt tot de derde generatie: systemen van nanosystemen. De vierde generatie in Roco’s model zullen moleculaire nanosystemen zijn, bijvoorbeeld kleine apparaatjes op moleculeschaal die vanaf de tekentafel ontwikkeld worden.

Biotechnologie

Tot de jaren zeventig van de vorige eeuw was de term biotechnologie vooral in zwang om voedingstechnologie, plantenveredeling en bio-industrie aan te duiden. Nadien werd de biotechnologie ook relevant als productietechniek voor de farmaceutische industrie en de geneeskunde waarbij recombinant DNA technologie en het kunstmatig kweken van weefsel niet meer zijn weg te denken

Tegenwoordig wordt de term biotechnologie vooral in de breedte gebruikt om alle methoden aan te duiden die organisch materiaal behandelen en bewerken met het oog op een toepassing voor mensen of dieren (als consument of als patiënt). De biotechnologie gaat dus veel verder dan gewasverdeling en veel toepassingen hebben een geneeskundig of therapeutisch oogmerk. Dit gegeven heeft ook de aandacht getrokken van

criminologen om te zoeken naar medicatie en therapieën [voor criminelen] vanuit een biologisch, biochemisch, neurobiologisch of biopsychiatrisch perspectief.

In de komende jaren zal de genetische analyse verder toenemen wat betreft snelheid van bepalingen en bedieningsgemak van apparatuur. Een denkbare toepassing zou het genenpaspoort kunnen zijn. Ook de synthetische biologie en synthetische geneeskunde waarbij materialen 'van de tekentafel' langs biotechnologische weg geproduceerd zouden kunnen worden, kan nieuwe producten opleveren om bijvoorbeeld de weerstand tegen ziektes te vergroten of ziekteverwekkers op hun zwakke plek aan te pakken of om de immuun respons die mensen van nature hebben kunstmatig te versterken. Biomedische productietechnieken zullen zich verder ontwikkelen in de richting van meer complexe kunstmatige weefselstructuren zoals kraakbeen. Gentherapie en het genetisch modificeren van menselijke genen zal in de toekomst een omvangrijk onderzoeksgebied blijven.

Hoeveel men ook heeft kunnen ontrafelen, het blijkt verrassend moeilijk om op basis van genetisch sporenmateriaal een voorspelling te doen over de uiterlijke kenmerken van de donor van dit materiaal. Het maken van een compositiefoto op basis van DNA gegevens is te complex voor de huidige stand van de wetenschap. Er zijn dan ook veel betere biologische aangrijpingspunten zoals hormoon- en proteïnespiegels waaruit afwijkingen in menselijk gedrag, gezondheid en lichamelijk functioneren gemakkelijker kunnen worden verklaard of voorspeld.

Informatietechnologie

Informatietechnologie omvat alle technologie die gerelateerd is aan het conceptueel of fysiek definiëren, ontwerpen of fabriceren van systemen en toepassingen voor gegevensverzameling, -opslag, -verwerking, -transport en beheer. Omdat inmiddels bijna alle aspecten van menselijk handelen sterk op ICT toepassingen berusten is het onmogelijk een alomvattend beeld te geven van de mogelijke toepassingen van ICT. We hebben in deze technologieverkenning alleen naar die toepassingen gekeken die we van belang achtten voor convergentie.

Op het niveau van toepassingen zien we momenteel een beweging in de richting van alomtegenwoordige intelligentie, slimme apparaten (bijvoorbeeld slimme wasmachines of slimme veiligheidsgordels die hun werking aanpassen wanneer dat nodig is). Bij systemen voor cameratoezicht zien we een steeds verdergaande groei van gegevens omdat er steeds meer steeds hoogwaardiger camera's zijn. Dit vraagt om methoden voor automatische herkenning (zowel identificatie als verificatie) van personen op basis van biometrische gegevens, en om methoden om die momenten te selecteren waar een menselijke observator van zulke monitorsystemen in het bijzonder naar zou moeten kijken. Autonomie is het kernbegrip bij veel toekomstige toepassingen van ICT. Een verregaand gebruik van robotica toepassingen in huishoudens is te voorzien. Er zijn toepassingen te verwachten om professionals die met grote hoeveelheden gegevens te maken hebben te bedienen met begrijpelijke visualisaties van die gegevens. De sensornetwerken zullen uiteindelijk ook op en in het lichaam gedragen kunnen worden en de activiteit in levende cellen kunnen volgen. Dankzij een toename van de kwaliteit van deze systemen zullen nieuwe complexe mechanismen blootgelegd worden. Maar deze systemen zullen ook vragen om verbeterde bedieningsmogelijkheden om hun werkelijke kracht te kunnen benutten.

Eén van de potentiële knelpunten rond ICT ligt in de vraag in hoeverre systemen blijvend in staat zijn om grote (en mogelijk sneller groeiende) volumina aan gegevens te hanteren. Een voorbeeld komt vanuit de biotechnologie. Een enkel menselijk genoom bevat al 6 Gigabit aan data. Ook de grote aantallen gegevens die beschikbaar zullen komen door de miljoenen zender-ontvangertjes (RFID labels) in logistieke stromen, en de groei van het aantal sensoren en zenders waardoor mensen op steeds eenvoudiger wijze communicatie over en weer hebben met computersystemen (bijvoorbeeld via spraaktechnologie) leiden tot sterk toenemende gegevensverzamelingen. De kwantumcomputer zou een oplossing voor dit gegevens explosieprobleem kunnen zijn. Omdat de rekenkracht van de kwantumcomputer verondersteld wordt om exponentieel toe te nemen met het aantal processoren (normale computers nemen lineair toe met het aantal processoren), zouden zij bij uitstek geschikt zijn voor het analyseren van zeer complexe combinatorische problemen. De vraag is echter of kwantum computers er komen en hoe lang dit nog zal duren.

Cognitieve technologie

Voor de doeleinden van dit document zijn de meest relevante aspecten van de cognitiewetenschap de studie van de structuren, functies en processen die aan de basis liggen van de menselijke perceptie, interpretatie van informatie, menselijke besluitvorming en ervaring van mentale toestanden.

Rekenkundige modellen van de menselijke waarneming gaan uit van een mathematische en algoritmische beschrijving van de neuronale processen. Deze theorieën werden ontwikkeld op basis van waarnemingen aan levende zenuwcellen die werden gestimuleerd, en de elektrofysiologische en MRI waarnemingen aan het brein van proefdieren en proefpersonen bij wie de zintuigen werden gestimuleerd (met bewegende beelden, geluidspatronen, etc.). Het menselijke brein zelf is te complex om in de huidige modellen afdoende te beschrijven vanuit zijn neuronale basis. Daarom zijn er naast de besproken rekenkundige ‘bottom up’ modellen over de werking van het brein ook veel ‘top down’ modellen die gebaseerd zijn op waargenomen menselijke (en dierlijke) gedragingen en ervaringen in allerhande situaties. Deze gedragsmodellen trachten een logisch verband te leggen tussen waargenomen gedrag en cognitieve toestanden. De theorieën over hogere orde cognitieve processen zoals mentale toestanden, ervaringen en bewustzijn zijn echter veelal op anekdotische waarnemingen gebaseerd en zijn soms zeer bedenkelijk. Daarnaast zijn binnen de kunstmatige intelligentie veel analytische, mathematisch logische, en statistische modellen voorgesteld om te verklaren hoe menselijk (en dierlijk) leren, redeneren, categoriseren, groeperen, ontdekken en herkennen van patronen, en relateren van gegevens plaatsvindt. Maar er bestaat rond die modellen maar weinig algemene instemming of zij de biologische intelligentie op een juiste manier verklaren.

Toekomstschouwers veronderstellen dat het menselijk verstand en menselijk bewustzijn voor 2020 zullen zijn ontrafeld, maar cognitiewetenschappers zijn daar zelf veel sceptischer over. Het ligt niet voor de hand dat hoog-niveau cognitieve functies zoals menselijke (en dierlijke) bedoelingen, creatieve manieren om problemen op te lossen, en bewustzijn volledig zullen zijn verklaard rond die datum. Breinwetenschappers vinden dat de verwachtingen voor het ‘uitlezen’ van de hersenen sterk overtrokken zijn. Een techniek zoals functionele MRI (fMRI) is bijzonder waardevol voor het opsporen van ziekten en afwijkingen, en ook breinstimulatie (in het brein of van buitenaf) lijkt bij de huidige stand van techniek al therapeutisch effect te hebben. Echter, het duurt nog lang

voordat het denkbaar is dat we met een manipulatie van buitenaf een specifieke gedachte of intentie kunnen aflezen of omgekeerd opwekken of onderdrukken.

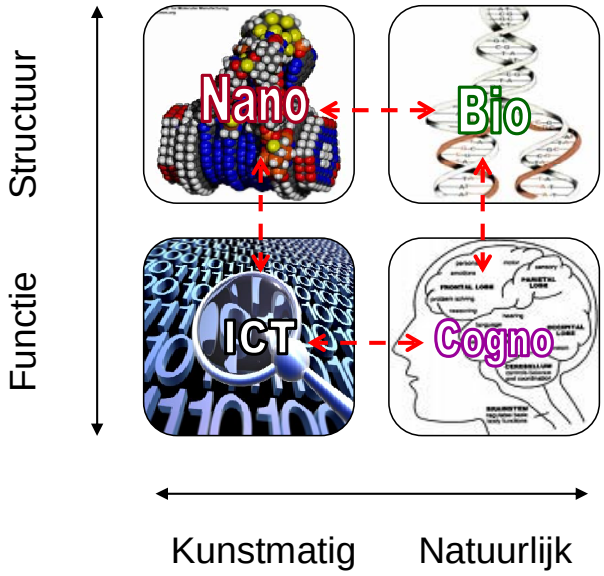
Toch lijken er binnen het vakgebied van de cognitiewetenschappen veel toepassingen in het maatschappelijke veiligheidsdomein mogelijk op basis van de inzichten die de wetenschap nu al heeft opgeleverd. Waarschijnlijk kunnen de inzichten in het automatisch analyseren en duiden van gelaatsexpressies veel ruimer worden ingezet om dreigende situaties te herkennen en vroegtijdig ingrijpen mogelijk te maken. Juist het vakgebied van de menselijke emoties is goed ontwikkeld en juist die emoties laten zich 'aflezen' zonder daarvoor aan de hersenen te hoeven meten. Ook eenvoudige bepalingen zoals concentratie van stresshormonen in het wangslijm vertellen veel over de stabiliteit en gemoedstoestand van een verdacht persoon. Samenvattend ontwikkelt de cognitiewetenschap zich snel in de richting van verregaand begrip van breinprocessen, maar zulke geavanceerde technieken zijn niet altijd praktisch of noodzakelijk, terwijl betrouwbare en bewezen technieken nog onderbenut blijven.

NBIC convergentie

Elk van de vier NBIC technologieën is op zichzelf al multidisciplinair. Daarom moeten we convergentie ook niet zien als een eigenschap van deze technologieën, maar meer als een proces. Dit proces kan leiden tot nieuwe paradigma's voor toepassingsgebieden. Deze doorbraken kunnen niet worden voorspeld. Niettemin vindt de convergentie logischerwijs plaats langs twee assen, structuur en functionaliteit, en wel als volgt (zie Figuur 35):

1 Nanotechnologie en biotechnologie hebben beide betrekking op *structuur*, weliswaar verschillend van aard, maar vergelijkbaar in (toekomstige) architecturale complexiteit.

2 Cognitie- en informatietechnologie hebben beide betrekking op functionaliteit werkend bovenop structuur van verschillende aard, met vergelijkbare (toekomstige) algoritmische complexiteit.



Figuur 35: Model voor een natuurlijke convergentie in twee richtingen.

Het belangrijkste effect van het convergentieproces is dat de verschillende technologieën verenigbaar worden en elkaar wederzijds versterken.

Toepassing van convergerende technologieën

Convergentie is een proces en wordt daarom zichtbaar via de toepassingen van technologie. Om een focus aan te brengen in de discussie over de betekenis van convergerende technologieën voor ons toepassingsdomein (maatschappelijke veiligheid), beperken we ons tot drie casussen:

- Casus 1: Het monitoren en volgen van voorwerpen en personen en het op afstand ingrijpen bij ongewenste bewegingen (afgekort: *Monitoren en ingrijpen*);
- Casus 2: Het verbeteren en ontwikkelen van forensisch sporenonderzoek (afgekort: *Forensisch onderzoek*);
- Casus 3: Het profileren, identificeren en monitoren van personen met een al dan niet verondersteld veiligheidsrisico (afgekort: *Profileren and identificeren*).

Voor elke casus schetsen we de verwachtingen op korte (5 jaar), middellange (10 jaar) of langere termijn (15 jaar).

Monitoren en ingrijpen heeft bijvoorbeeld betrekking op plaatsbepaling- en/of communicatietechnologie (zoals GPS of RFID) die kan worden gebruikt om objecten of personen op te sporen en te volgen. Een bijzonder geval hiervan is het voorzien van personen van een elektronisch label, zoals op dit moment experimenteel gebeurt met gevangenen. Personen kunnen ook worden opgespoord of gevolgd met het oog op hun eigen veiligheid. In het algemeen blijkt men bereid hier privacy in te leveren omwille van de eigen of collectieve veiligheid, al blijft privacy niet onbelangrijk. Voor het monitoren en (het op afstand) ingrijpen wordt momenteel vooral informatietechnologie gebruikt. Convergerende technologieën zullen het mogelijk maken dat vele variabelen (denk ook aan sensoren in het lichaam of op de huid) online worden bijgehouden of gestuurd, en daarmee tot betere risicoanalyse of manieren van ingrijpen. Daarbij is wel aandacht nodig voor het eventueel ‘knoeien’ met de technologie. In onze toekomstverkenning geven we aan dat de volgende toepassingen op het gebied van monitoren en ingrijpen als technische werkelijkheid haalbaar zullen zijn in 2022:

– Individuele sensoren. In het bijzonder het labellen van gevangenen of TBS'ers met een geïmplanteerde RFID chip (korte termijn).
– Persoonlijke, draagbare apparaten met gegevensopslag en online communicatie mogelijkheden (korte termijn).
– Traceren en volgen van individuen in stedelijke gebieden.
– Implantaten (of prothesen) die menselijke biologische functies verbeteren (respectievelijk nabootsen), echter geen selectief wissen van herinneringen en geen gedragsmanipulatie via hersenimplantaten.
– Het op basis van sensor informatie automatisch ingrijpen (bijvoorbeeld blokkeren) bij (rijdende) auto's (korte termijn).
– Objecten (zoals kleding) die reageren op externe signalen (zoals locatie, hartslag, etc.).
– Draadloos Internet wereldwijd beschikbaar (korte termijn).

In het forensisch sporenonderzoek ontstaan nieuwe of radicaal verbeterde manieren van werken en bewijsvoering. Een voorbeeld is al het gebruik van DNA voor identificatiedoeleinden. Nieuwe technologieën zullen ook nodig zijn om minieme sporen (op het niveau van moleculen) te kunnen analyseren. Convergerende technologieën leiden ertoe dat zelfs de werkwijzen zullen veranderen. Snelle analyseresultaten ter plaatse via lab-on-a-chip technologie, bijvoorbeeld, zullen het zoeken naar sporen direct beïnvloeden. De miniaturisatie en comodificatie van technologie leidt er bovendien toe dat analysetechnieken beschikbaar komen voor het grote publiek, waar voorheen alleen gespecialiseerde instituten hierover beschikten. Betrokkenheid van burgers bij het verzamelen van informatie neemt toe door ontwikkelingen als weblog's en internetgemeenschappen. De relevante technologie voor de komende jaren omvat draagbare analyse-instrumenten, grootschalige gegevensbanken, het detecteren een enkele molecule, biomarkers, DNA profielen en 3D visualisatie van de plaats delict. In onze toekomstverkenning geven we aan dat de volgende toepassingen op het gebied van forensische opsporing als technische werkelijkheid haalbaar zullen zijn in 2022:
– Snelle forensische analyse op basis van zeer kleine hoeveelheden materiaal (korte termijn).
– Het gebruik van nieuwe generaties kleine, selectieve, hooggevoelige en nauwkeurige biologische sensoren.
– Het commercieel beschikbaar komen (comodificatie) van lab-on-a-chip technologie.
– Objecten (zoals kleding) die reageren op de aanwezigheid van geringe hoeveelheden specifieke stof.
– Krachtige draagbare computer / mobiele laboratoria (korte termijn).
– Driedimensionale visualisatie van de plaats delict.
– Textiel dat bestand is tegen sporen, waar geen sporen op hechten (lange termijn).

Voor het zoeken naar personen met een al dan niet verondersteld veiligheidsrisico kan een risicoprofiel worden opgesteld ('profiling'). Op basis van alle beschikbare informatie vindt dan een risicoanalyse plaats. Profiling is daarmee ook het voorspellen van (of anticiperen op) gedrag dat men verwacht op basis van alle beschikbare informatie. Identificatie betreft het herkennen van een specifieke persoon – van wie de identiteit bekend is – in de menigte. Personen laten steeds meer sporen na: door het surfen op Internet, door het gebruik van hun mobiele telefoon, door het bij zich dragen van RFID labels, of door te worden geobserveerd door camera's. De hoeveelheid data die voor een persoon of voorwerp wordt geregistreerd groeit gigantisch. Dit kan worden gebruikt bij deze casus (profiling en identificatie), waarin informatieverwerking en gezichtherkenning een belangrijke rol spelen. Het lezen van gedachten is echter nog ver weg, en ook het afleiden van verwacht gedrag uit iemands genen is niet iets dat de

komende 15 jaar toepasbaar is. Niettemin zal het samenvoegen van informatie uit allerlei sensoren in en op het lichaam, en uit cognitieve analyses het mogelijk maken risico's te voorspellen. In onze toekomstverkenning geven we aan dat de volgende toepassingen op het gebied van profiling en identificatie als technische werkelijkheid haalbaar zullen zijn in 2022:

- Grootschalig gebruik van cameratoezicht en observatie van personen en omgevingen / aanwezigheid van sensoren in de publieke ruimte.
- Onopvallend cameratoezicht en 'onzichtbare' sensornetwerken met sensoren van steeds kleinere omvang (korte tot middellange termijn).
- Grootschalig gebruik van RFID labels (bijvoorbeeld in de retail sector), welke tevens kunnen worden gebruik om personen te volgen (korte termijn).
- Omvangrijke gegevensbanken, bijvoorbeeld met informatie over ieders genoom (korte termijn).
- Koppelen van informatiebronnen (gegevensbanken, sensorinformatie), en toegenomen zoekmogelijkheden en kunstmatige intelligentie om deze informatie te verwerken.
- Brede toepassing van biometrie –waarschijnlijk gecombineerd met andere beschikbare context informatie– voor veiligheidstoepassingen (maar niet het lezen van gedachten).
- Verbeterde en op spraak gebaseerde mens-machine interactie, waardoor snel en onopvallend heel veel informatie digitaal kan worden vastgelegd.
- Genetisch screenen voor pathologische doeleinden, maar niet voor het voorspellen van verwacht gedrag.
- Security technieken die anonimiteit op bijvoorbeeld Internet of bij transacties (betalingen) mogelijk maken.

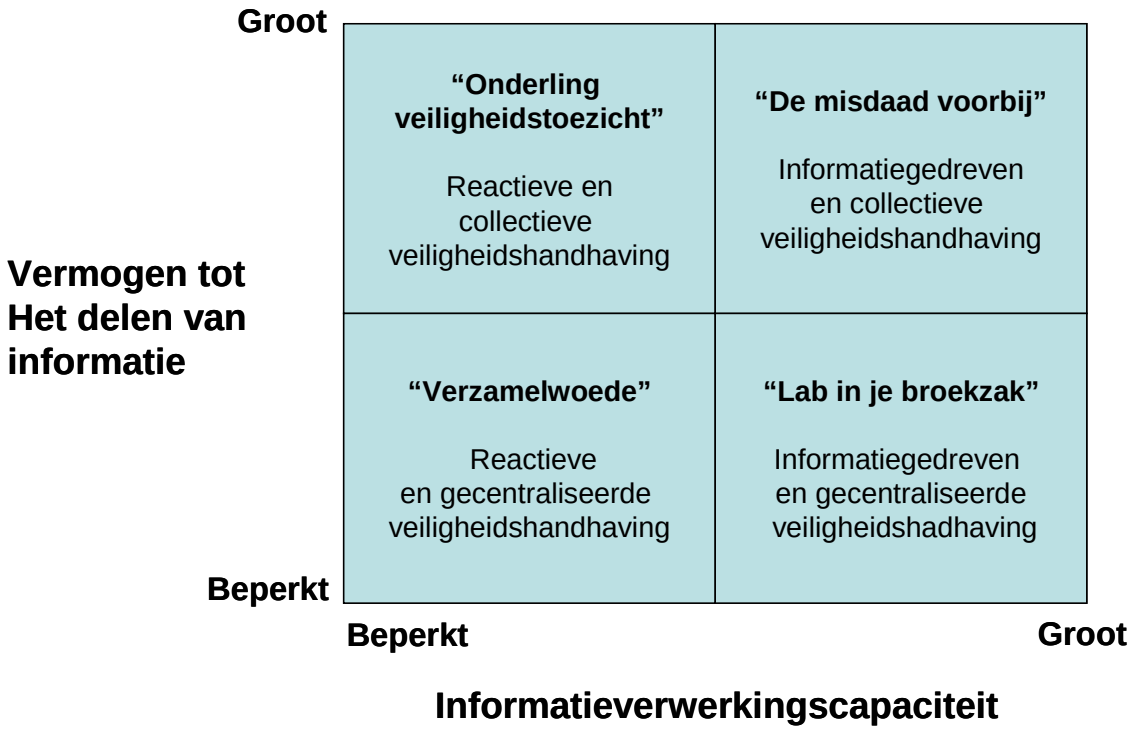
Scenario's

We hebben vier scenario's geschetst om de toekomstige toepassing van convergerende technologieën binnen ons toepassingsdomein te visualiseren. De scenario's zijn gebaseerd op de te verwachten (realistische) technologieontwikkelingen voor de komende 15 jaar. De scenario's zijn geschreven vanuit een technologisch gezichtspunt en worden tevens gebruik als middel om een impactanalyse mogelijk te maken. Om te komen tot vier gerelateerde, karakteristieke scenario's is gebruik gemaakt van twee onzekerheden voor de toekomst:

1 Het delen van informatie: de mate waarin we in staat zijn om informatie adequaat te delen tussen alle betrokkenen in de veiligheidsketen.
2 Het verwerken van informatie: de mate waarin we in staat zijn de steeds groeiende gegevensstroom op te slaan en te analyseren.

In alle scenario's schetsen we een ontwikkeling waarin technologie 'onzichtbaar' wordt, wat resulteert in een verschuiving naar wat we hebben genoemd een 'omgevende en intelligente publieke veiligheidshandhaving'. Afhankelijk van hoe de twee onzekere factoren zich ontwikkelen (in de scenario's kiezen we voor de extremen in beperkte mate / in grote mate) zijn vier toekomstscenario's mogelijk (zie Figuur 36). Deze scenario's hebben we de karakteristieke typeringen 'De misdaad voorbij', 'Onderling veiligheidstoezicht', 'Lab in je broekzak'en Verzamelwoede' gegeven. 'Verzamelwoede' kenmerkt zich door het verzamelen van informatie of bewijs en dit naar behoefte achteraf gebruiken. In 'De misdaad voorbij'zien we een verschuiving van een dergelijke reactieve overheid naar een proactieve overheid, die technologie gebruikt om te anticiperen op gebeurtenissen en misdaad te voorkomen. De technologie is hierbij ondersteunend aan de trend richting preventie. De twee andere scenario's richten zich meer op specifieke

toepassingen, en tonen hoe convergerende technologieën een drijfveer voor nieuwe paradigma's in het veiligheidsveld kunnen zijn. Burgers krijgen een veel actievere rol in het forensisch onderzoek ('Lab in je broekzak') respectievelijk bij toezicht en handhaving ('Onderling veiligheidstoezicht').



Figuur 36: Het gebruik van twee kernonzekerheden om vier gerelateerde scenario's op te spannen.

Het scenario 'de misdaad voorbij' is sterk gerelateerd aan de casus rond profiling en identificatie. Het toont de tendens naar preventie, een verschuiving van een reactieve naar een informatiegedreven omgeving. Sensoren zijn overal aanwezig en de informatie kan goed worden verwerkt om de juiste beslissingen te nemen. Het overheidsbeleid is gericht op anticipatie en het voorkomen van criminaliteit. Karakteristieken van de toekomstige situatie zijn:

- Er wordt online toezicht gehouden op personen met een al dan niet verondersteld veiligheidsrisico;
- Grootschalig gebruik van RFID labels in of op het lichaam voor toezicht- of identificatiedoeleinden;
- Het gebruik van sensoren (cameratoezicht, sensoren op het lichaam, hersenscans, etc.) voor bijvoorbeeld agressiedetectie;
- Het koppelen van publieke en private informatiebronnen met het oog op een alomvattende analyse van iemands gedrag en zijn relaties met anderen;
- Actuatoren via welke personen kunnen worden beperkt in hun bewegingsvrijheid.

Het scenario 'onderling veiligheidstoezicht' is sterk gerelateerd aan de casus rond monitoren en ingrijpen. Het scenario toont een paradigmaverandering rond (publiekprivate) samenwerking. Door samenwerking met private partners en burgers wordt het mogelijk om op kleinschalige, individuele basis iemand te volgen en te observeren. Dit maakt therapie in de eigen vertrouwde omgeving mogelijk ('gevangenis zonder muren'). Karakteristieken van de toekomstige situatie zijn:

– Individueel volgen en observeren van personen een naadloze overdracht tussen systemen buitenshuis (GPS) en binnenshuis (cameratoezicht), en tussen publieke en private systemen;
– De gehele bevolking wordt preventief gescand op aanleg voor crimineel gedrag;
– Een steeds onscherper onderscheid tussen de virtuele en de werkelijke wereld;
– Burgers dragen bij aan het volgen van criminelen en het handhaven van de wet; onderling toezicht en sociale controle tussen burgers.

Het scenario 'lab in je broekzak' is sterk gerelateerd aan de casus rond forensisch onderzoek. Het scenario toont een paradigmaverandering rond de beschikbaarheid van specialistische apparatuur voor de gewone burger. De hulpmiddelen om bijvoorbeeld sporen te analyseren worden klein, snel, nauwkeurig, goedkoop en gebruikersvriendelijk. Daarmee sturen (en dus veranderen) de analyseresultaten ook het hele (forensische) onderzoeksproces. Dergelijke hulpmiddelen worden algemene producten die ook beschikbaar komen voor private onderzoekers of criminelen. Karakteristieken van de toekomstige situatie zijn:
– Nano spuitbussen waarmee de kleinste sporen kunnen worden ontdekt;
– 3D reconstructie van de plaats delict;
– Lab-on-a-chip technologie is beschikbaar voor iedereen;
– Sensorinformatie van over de hele wereld komt als een dienst beschikbaar voor burgers (traceren locaties, camerabeelden, etc.);
– Real-time analyse van gegevens, bijvoorbeeld voor treffers in gegevensbanken (DNA, gezichtsherkenning), voor sporenonderzoek, etc.

Het scenario 'verzamelwoede' is niet specifiek gerelateerd aan één van de drie casussen. Het scenario extrapoleert de huidige, enigszins reactieve (eerder dan anticipatieve) processen naar de toekomst. Dit betekent echter niet dat dit scenario minder geavanceerd is: de NBIC technologie heeft wel vooruitgang geboekt. Karakteristieken van de toekomstige situatie zijn:
– Er wordt heel veel informatie vergaard, geordend, gepresenteerd, etc. Deze gegevens worden vooral achteraf gebruikt;
– Werkzaamheden verschuiven van publieke naar private partners en uiteindelijk naar de burger, steeds echter op basis van dienstverlening eerder dan samenwerking;
– Technologie rond cameratoezicht is sterk verbeterd, waardor het bijvoorbeeld mogelijk is een onderscheid te maken tussen vrijwillig of gedwongen gedrag.

Impact analyse

De technologische ontwikkelingen, de toepassingen en scenario's roepen uiteraard ook allerlei maatschappelijke en normatieve vragen op. De manier waarop de impact van de technologische ontwikkelingen in dit rapport bestudeerd en geanalyseerd wordt, is er één van vele mogelijke. Bij de analyse en evaluatie van de mogelijke consequenties van technologische ontwikkelingen zijn die technologische ontwikkelingen als op zichzelf staande factoren verondersteld, waarbij de mogelijke toekomstige wisselwerking met maatschappelijke en normatieve ontwikkelingen buiten beschouwing is gelaten. Dat betekent dat de hier gegeven impactanalyse indicatief is en geen vastomlijnd beeld geeft van een vaststaande toekomst. De bedoeling is vooral om aandacht te vestigen op mogelijke problemen en dilemma's die aandacht verdienen.

Acht maatschappelijke en normatieve trends kunnen het gebruik van convergerende technologieën voor veiligheidsdoeleinden beïnvloeden. In de praktijk zullen deze trends

elkaar vaak overlappen. Wij onderscheiden vier maatschappelijke en vier ethische en juridische trends:

Maatschappelijk
1 Er zullen steeds meer gegevens over mensen worden opgeslagen. Ook zullen deze breder worden verspreid. De mensen over wie de gegevens gaan zullen het moeilijker krijgen om controle uit te oefenen. De overheid zal gemakkelijker toegang krijgen tot de gegevens. De mogelijkheid van publieke en private partijen om inzicht te krijgen in het doen en laten van de burger – met inbegrip van terroristen, criminelen én de 'doorsnee burger' – groeit exponentieel.
2 Verschuivingen in de methoden van observatie en toezicht leiden in toenemende mate tot normaliserings- en disciplineringseffecten op gedrag, zelfperceptie, persoonlijkheid en levensvisie.
3 Regulering wordt meer en meer gedelegeerd van personen naar technologie, en van publieke, gouvernementele partijen naar private organisaties en burgers.
4 Door de groeiende complexiteit en onzekerheid zullen de beleidsvorming over en de bestuurbaarheid van technologie zelf aanzienlijk worden bemoeilijkt.

Ethisch en juridisch
1 Nieuwe mogelijkheden van observatie en toezicht vertonen zowel centralisatie- als decentralisatietendensen (die elkaar niet neutraliseren). Daarnaast worden de instrumenten voor observatie en toezicht zelf steeds onopvallender. Door deze drie ontwikkelingen veranderen de aard en de perceptie van privacyinbreuken.
2 Het doel en het bereik van het strafrecht verschuift van reactie, vergelding en rehabilitatie naar preventie en risicobeheersing.
3 Opvattingen over persoonlijke vrijheid en verantwoordelijkheid zullen veranderen. Zelfcontrole zal steeds vaker plaats maken voor controle door anderen. Deze veranderingen zullen van invloed zijn op het beeld van de eigen identiteit en de identiteit van anderen. Zij ondermijnen echter niet noodzakelijk de opvattingen van recht en moraal die persoonlijke vrijheid en verantwoordelijkheid van mensen vooronderstellen.
4 Het steeds meer inbouwen van normen en hun handhaving in technologie die gedrag beïnvloedt zal zich steeds moeilijker verdragen met bepaalde opvattingen van moraal en recht waarin intrinsieke waarde wordt toegekend aan de mogelijkheid van mensen om er in vrijheid voor te kiezen het goede en het juiste te doen. Daarnaast zal zij vragen gaan oproepen omtrent de legitimiteit van de geïncorporeerde regulerings- en handhavingsarrangementen.

Met de technologie ontwikkelen zich natuurlijk ook normatieve kaders en paradigma's. Sommige van deze veranderingen komen naar voren in bovengenoemde trends. Uiteraard kunnen de trends zelf ook gezien worden als aanvullend element in de scenario's. Technologische ontwikkelingen hebben maatschappelijke en normatieve consequenties. Omgekeerd hebben maatschappelijke en normatieve ontwikkelingen ook hun invloed op de technologie. Bij een impactanalyse moet dit goed voor ogen worden gehouden. Zowel de technologie als de maatschappelijke en normatieve kaders kunnen veranderen in het verloop van deze co-evolutie.

In een addendum bij dit rapport worden de scenario's en trends geconfronteerd met de normatieve uitgangspunten van het bestaande Nederlandse (straf-)recht. Hierbij moet bedacht worden dat een dergelijk normatief kader niet voor eeuwig vastligt: Ook dit kader is aan veranderingen onderhevig. Daarom is ervoor gekozen deze confrontatie te presenteren als aanzet tot het denken en discussiëren over de betekenis van de geschetste technologische ontwikkelingen. Deze aanzet kan leiden tot nader onderzoek en debat, waarbij keuzes en afwegingen gemaakt zouden kunnen worden over de wisselwerking tussen de technologische ontwikkelingen en de maatschappelijke en normatieve kaders.

References

Anderson, J. R. (1993), *Rules of the Mind*, Hillsdale, NJ: Erlbaum.

Bainbridge, W.S. & Roco, M.C. (Eds) (2006), *Managing Nano-Bio-Info-Cogno Innovations: Converging Technologies in Society*, Springer.

Beck, U. (1999), *World risk society*, Malden, MA: Polyty Press

Behringer, R.R., Ryan, T.M., Reilly, M.P., Asakura, T., Palmiter, R.D., Brinster, R.L., & Townes, T.M. (1989), Synthesis of functional human hemoglobin in transgenic mice, *Science*, *245 (4921)*, 971-973.

Bentham, J. (1843), *Jeremy Bentham: Collected Works (*ed. J. Bowring), London.

Blobel, G., & Sabatini, D.D. (1971), Ribosome-membrane interactions in eukaryotic cells, In L.A. Manson (ed.), *Biomembranes* New York: Plenum Publishing Corporation (193-195)

Blok, P. (2002), *Het recht op privacy*, Den Haag: Boom Juridische uitgevers.

Borgers, M.J. (2007), *De vlucht naar voren*, oratie Amsterdam (VU), Den Haag: Boom Juridische uitgevers

Brenner, S.W. (2004), Distributed Security: Moving Away From Reactive Law Enforcement, *International Journal of Communications Law & Policy* (9).

Browne, W.R., & Feringa, B.L. (2006), Making Molecular Machines Work, *Nature Nanotechnology*, *1* 33.

Brownsword, R. (2004), What the World Needs Now: Techno-Regulation, Human Rights and Human Dignity, in: R. Brownsword (ed.), *Global Governance and the Quest for Justice, Vol. 4: Human Rights*, Oxford: Hart 2004 (203-234)

Brunner, H. G., Nelen, M., Breakefield, X. O., Ropers, H. H. & van Oost, B. A. (1993), Abnormal behavior associated with a point mutation in the structural gene for monoamine oxidase A, *Science 262* 578–580

Capecchi, M. R. (1989), Altering the genome by homologous recombination, *Science 244*, 1288-1292.

CBD/COGEM/Gezondheidsraad (2007), *Trendanalyse biotechnologie 2007 kansen en keuzes* Joint memorandum (in Dutch) by the Commission for Animal Biotechnology (CBD), the Commission Genetic Modification (COGEM), and the National Health Council, Utrecht: 2007.

Chalmers, D. (1996), *The Conscious Mind: In Search of a Fundamental Theory*, Oxford University Press.

Choi, S., Ban, S., & Lee, M. (2004), Biologically Motivated Visual Attention System Using Bottom-Up Saliency Map and Top-Down Inhibition, *Neural Information Processsing Letters & Review 2 (1)*.

Crick, F., & Koch, C. (1990), 'Towards a neurobiological theory of consciousness', *Seminars in the Neurosciences*, *2*, 263-275.

Corstens, G. (1995), *Het Nederlands strafprocesrecht*, Arnhem: Gouda Quint

Custers, B.H.M. (2001), Data Mining and Group Profiling on the Internet. In: A.H. Vedder (ed.), *Ethics and the Internet*. Antwerpen, Groningen, Oxford: Intersentia, (87-104)

Custers, B. (2004), *The Power of Knowledge. Ethical, Legal, and Technological Aspects of Data Mining and Group Profiling in Epidemiology*, Nijmegen: Wolf Legal Publishers

De Bruijn, H., Van der Voort, H., Dicke, W., De Jong, M. & Veeneman, W. (2004), *Creating System Innovation*, Leiden: A.A. Balkema Publishers

Dennett, D.C. (1991), *Consciousness Explained,* London: Little, Brown & Co

Dennett, D.C. (2003), *Freedom Evolves*, New York: Viking Books

Doorn, M. (Ed.) (2006), *Converging Technologies*, STT Netherlands Study Centre for Technology Trends.

Dorbeck-Jung, B.R. (1998), Towards Reflexive Responsibility. New Ethics for Public Adminstration, in: A. Hondeghem (ed.), *Ethics and Accountability in a Context of Governance and New Public Administration*, Amsterdam-Washington (45-58)

Dorbeck-Jung, B.R. (2006), Coping with the complexity, uncertainty and ambiguity of risk problems related to nanotechnologies development – how can public regulation be developed in a process of reflective learning? Contribution to the ECPR/CRI Conference, Bath, September 7-9.

Dorbeck-Jung, B.R. (2007), What can other governments learn from the United Kingdom's regulatory activities related to nanotechnologies? What can other governments learn from the United Kingdom's regulatory activities related to nanotechnologies?, Paper presented at a Conference of Basel University, May 5-7.

Dorbeck-Jung, B.R. (2008), Challenges to the legitimacy of international regulation – the case of pharmaceuticals standardisation, forthcoming in A. Follesdal, R. Wessel & J. Wouters (eds.), *Multi-level regulation and the EU.* Leiden: Martinus Nijhoff Publishers, 2008

Doreleijers, T.A.H. (1998), De dokter en de zware jongen; over de behandeling van jongeren met psychiatrische stoornissen die misdrijven begaan, *Medisch Contact 53 (17)* 581-585.

Drexler, E. (2003a), Open Letter to Richard Smalley, *Chemical & Engineering News*, *81*, 38-39.

Drexler, E. (2003b), Drexler Counters, *Chemical & Engineering News*, *81*, 40-41.

Engel, A.K., Fries, P., & Singer, W., (2001), Dynamic Predictions: Oscillations and Synchrony in Top-down Processing, *Nature*, *2*, 704-716.

European Technology Assessment Group ETAG (2006), *Technology assessment on converging technologies*, Report IP/A/STOA/ST/2006-6 Policy Department Economic and Scientific Policy, European Parliament, October 2006.

Foucault, M. (1977), *Discipline and Punish: The Birth of Prison*, New York: Pantheon.

Garland, D. (2001), *The culture of control: crime and social order in contemporary society*, Chicago: University of Chicago Press.

Geim, A.K., & Novoselov, K.S. (2007), The Rise of Graphene, *Nature Materials, 6*, 183-191.

Gesch, C.B., Hammond, S.M., Hampson, S.E., Eves, A., & Crowder, M.J. (2002), Influence of supplementary vitamins, minerals and essential fatty acids on the antisocial behaviour of young adult prisoners: Randomised, placebo-controlled trial, *The British Journal of Psychiatry*, *181*, 22-28.

Gill, P., Jeffreys, A.J., & Werrett, D.J. (1985), Forensic application of DNA 'fingerprints', *Nature, 318* , 577 - 579.

Gorbis, M., & Pescovitz, D., (2006), Bursting Tech Bubbles Before They Balloon, *IEEE Spectrum*, September 2006, 42 – 47.

Goffman, E. (1963), *Stigma: Notes on the Management of Spoiled Identity*, New York: Simon and Schuster.

Gordon, C. (1991), Governmental Rationality, in: G. Burchell et al. (eds.), *The Foucault Effect,* Hemel Hemstead: Harvester Wheatsheaf,.(1-51)

Gordon, D. (1987), The Electronical Panopticon: A case study of the development of the national criminal records system, *Politics and Society, 15 (4)*. 483-499.

Gutwirth, S. & De Hert, P. (2005), Privacy and Data Protection in a Democratic Constitutional State, in: M. Hildebrandt & S. Gutwirth (eds.), *D7.4: Implications of profiling practices on democracy and rule of law*: FIDIS**,** 11-28.

Gyselinckx, B., Van Hoof, C., Ryckaert, J., Yazicioglu, R.F., Fiorini, P., &. Leonov, V. (2005), *Human++: Autonomous Wireless Sensors for Body, Area Networks*, IEEE 2005 Custom Integrated Circuits Conference.

Harris, P. (2007), *An introduction to law* 7th Ed, Cambridge: Cambridge University Press.

Harteveld, A.E., Keulen, B.F. & Krabbe, H.G.M. (1996), *Het EVRM en het Nederlandse strafprocesrecht*, Groningen: Wolters Noordhoff

Hawkins, J., & George, D. (2006), *Hierarchical Temporal Memory. Concepts, Theory, and Terminology*, Menlo Park: Numenta Inc., http://www.numenta.com/Numenta_HTM_Concepts.pdf.

Hebb, D.O. (1949), *The Organization of Behavior: A Neurophysiological Theory,* New York: John Wiley & Sons Inc.

Heisenberg, W. (1927) Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik, *Zeitschrift für Physik*, *43*,172-198.

Hochberg, L.R., Serruya, M.D., Friehs, G.M., Mukand, J.A., Saleh, M., Caplan, A.H., Branner, A., Chen, D., Penn, R.D., & Donoghue, J.P. (2006), Neuronal ensemble control of prosthetic devices by a human with tetraplegia, *Nature 442*, 164-171.

Hoven van den, J., & Vermaas, P.E., (2007), Nano-Technology and Privacy: On Continuous Surveillance outside the Panopticon, *Journal of Medicine and Philosophy, 32* 283-297.

Hubel, D.H., & Wiesel, T.N., (1962), 'Receptive fields, binocular interaction and functional architecture in the cat's visual cortex', *Journal of Physiology,* 160, 106-154.

Hunt, A., & Wickham, G., (1994), *Foucault and the Law,* London: Pluto Press.

Information Technology for European Advancement (ITEA) (2004), *Technology roadmap for software intensivce systems,* 2nd edition, May 2004, ITEA Office, Eindhoven, The Netherlands, http://www.itea-office.org/itea_roadmap_2.

International Risk Governance Council (IRGC) (2006), *Nanotechnology, risk governance*, White paper no. 2, IRGC, Geneva.

Itti, L., Koch, C. & Niebur, E., (1998), A model of saliency-based visual attention for rapid scene analysis, *IEEE Transactions on Pattern Analysis and machine Intelligence*, *20(11)*, 1254-1259.

Jeffreys, A.J., Wilson, V. , & Thein , S.L., (1985a), Hypervariable 'minisatellite' regions in human DNA, *Nature 314*, 67-73.

Jeffreys, A.J., Wilson, V. , & Thein , S.L., (1985b), Individual-specific 'fingerprints' of human DNA, *Nature 316*, 76-79.

Kimpton, C.P., Gill, P., Walton, A., Urquhart, A., Millican, E.S., & Adams, M. (1993), Automated DNA profiling employing multiplex amplification of short tandem repeat loci, *PCR Methods Appl. 3*. 13-22.

Klip, A.H. (2004), *Uniestrafrecht*, oratie Maastricht, Deventer: Kluwer

Koller, B.H., Hagemann, L.J., Doetschman, T., Hagaman, J.R., Huang, S., Williams, P.J., First, N.L., Maeda, N., & Smithies, O. (1989), Germ-line Transmission of a Planned Alteration Made in a Hypoxanthine Phosphoribosyltransferase Gene by Homologous Recombination in Embryonic Stem Cell, *Proc. Natl. Acad. Sci. 86*, 8927-8931.

Koopmans, F.A.J. (1997), *Het beslissingsmodel van 348/350 Sv*. Groningen: Wolters-Noordhoff.

Koops, B.J. (2006), *Tendensen in opsporing en technologie. Over twee honden en een kalf*, oratie Tilburg, Nijmegen: Wolf Legal Publishers

Koops, B.J. (ed.) (2004), *Strafrecht en ICT*, (Monografieën Recht en Informatietechnologie), Den Haag: Sdu.

Koops, B.J. & Groothuis, M.M. (2007), Constitutional Rights and New Technologies in the Netherlands, in: R. Leenes & B.J. Koops (red.), *Constitutional Rights and New Technologies*, The Hague: T.M.C. Asser Press

Koops, B.J., Buitelaar, H., & Lips, M. (eds.), *D5.4: Anonymity in electronic government: a case-study analysis of governments' identity knowledge*, FIDIS Deliverable, May 2007, available at http://www.fidis.net/fidis-del/.

Kruissink, M., Post, B. & Stoltz, S. (2007), De gevangenis van de toekomst?, *Justitiële verkenningen*, *33 (4)*, 44-59. http://www.wodc.nl/images/JV0704_artikel03_tcm44-79852.pdf

Kyle, J.W., Birkenmeier, E.H., Gwynn, B., Vogler, C., Hoppe, P.C., Hoffmann, J.W., & Sly, W.S. (1990), Correction of Murine Mucopolysaccharidosis VII by a Human ß- Glucuronidase Transgene, *Proceedings of the National Academy of Sciences*, *87*, 3914-3918.

Laplace, P.S. (1840), *Essai philosophique sur les probabilités*, Paris: Bachelier.

Leenes, R., & Prins, J.E.J. (2006), Techniek als alternatief reguleringsinstrument, implicaties voor privaatrechtelijke verhoudingen. In: B. Dorbeck-Jung & M. Oude Vrielink-van Heffen, *Op weg naar bruikbare regulering?* Themanummer *Recht der Werkelijkheid*, p. 117-134.

Leenes, R., & Koops, B.J. (eds.) (2007), *Constitutional Rights and New Technologies. A Comparative Study Covering Belgium, Canada, France, Germany, the Netherlands, Sweden, and the United States*, (IT & Law Series), The Hague: T.M.C. Asser Press.

Lehn, J.-M. (1990), Perspectives in Supramolecular Chemistry - From Molecular Recognition towards Molecular Information Processing and Self-Organization, *Angewandte Chemie International Edition in English*, *29,(11)*, 1304-1319, DOI: 10.1002/anie.199013041.

Llinás, R.R., Walton, K.D., Nakao, M., Hunter, I.W., & Anquetil, P.A., (2005), Neuro-vascular central nervous recording/stimulating system: using nanotechnology probes, *Journal of Nanoparticle Research*, 7 (2-3), 111-127.

Loewi, O., (1921), Über humorale übertragbarkeit der Herznervenwirkung, *Pflügers Archiv*, *189(1)*, 239-242.

Lømo, T. (2003), The discovery of long-term potentiation, *Philos Trans R Soc Lond B Biol Sci, 358 (1432)*, 617–20.

Lyon, D. (1993), An electronical panopticon? A sociological critique of surveillance theory, *The Sociological Review, 41 (4)*, 653-678.

Lyon, D. (2002) *Surveillance society : monitoring everyday life*, Philadelphia: Open University Press.

Marr, D. (1982), *Vision: A computational investigation into the human representation and processing of visual information*, Henry Holt & Co

Mazzone, A., Zhang, R., & Kunz, A. (2003), Novel actuators for haptic displays based on electroactive polymers, In *Proceedings of the ACM Symposium on Virtual Reality Software and Technology (Osaka, Japan, October 01 - 03, 2003)*, VRST '03. New York: ACM Press, 196-204, http://doi.acm.org/10.1145/1008653.1008688

Mehta, M. (2002), Privacy versus Surveillance. How to avoid a nano-panoptic future, *Canadian Chemical News*,.31-33.

Mehta, M. (2003), *On Nano-Panoptocism. A Sociological Perspective*, available at: http://chem4823.usak.ca/

Microsoft Research (2005), *Towards 2020 Science*, Cambridge: Microsoft, http://research.microsoft.com/projects/cambridge/2020Science/downloads/T2020S_ReportA4.pdf.

Mohamed, F.B., Faro, S.H., Gordon, N.J., Platek, S.M. , Ahmad, H., & Williams, J.M. (2006), Brain Mapping of Deception and Truth Telling about an Ecologically Valid Situation: Functional MR Imaging and Polygraph Investigation—Initial Experience, *Radiology 238*, 679-688.

Moodera, J.S., & Mathon, G. (1999), Spin polarized tunneling in ferromagnetic junctions, *Magn. Magn. Mater. 200*,. 248-273.

Mullis, K., Faloona, F., Scharf, S., Saiki, R., Horn, G., & Erlich, H. (1986), Specific enzymatic amplification of DNA in vitro: the polymerase chain reaction, *Cold Spring Harb.Symp.Quant.Biol. 51*, 263-273.

Murakami Wood, D. (ed.) (2006), *A Report on the Surveillance Society. For the Information Commissioner by the Surveillance Studies Network*, September 2006 http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf.

Neild, I., & Pearson, I., (eds.) (2005), *2005 BT Technology Timeline*.

Newell, A. (1990), *Unified Theories of Cognition*, Harvard University Press.

Nissenbaum, H. (2004), Privacy as contextual integrity, *Washington Law Review*, *79*, 119-132.

Nordmann, A. (2004), *Converging Technologies – Shaping the future of European societies*, Report European Commission Research, http://www.ntnu.no/2020/pdf/final_report_en.pdf.

Nordmann, A. (2007), If and Then: A Critique of Speculative NanoEthics, *Nanoethics 1*: 31-46.

Nouwt, J. (1997), *Zorg voor privacy; informatietechnologie en informationele privacy in de gezondheidszorg*; Den Haag: SDU Uitgevers.

Oberdörster E. (2004), Manufactured Nanomaterials (Fullerenes, C_{60}) Induce Oxidative Stress in the Brain of Juvenile Largemouth Bass, *Environmental Health Perspectives 112(10),* 1058–1062.

OECD (2005), *Statistical Definition Of Biotechnology*, updated in 2005, www.oecd.org

Omkins, P.L. (1998), Panopticon: Technology, the individual and social control in the early 21st century, *RUSI Journal*, 51-59.

Palmiter, R.D., Brinster, R.L., Hammer, R.E., Trumbauer, M.E., Rosenfeld, M.G., Birnberg, N., & Evans,R., (1982), Dramatic growth of mice that develop from eggs microinjected with metallothionein−growth hormone fusion genes, *Nature 300*, 611 – 615.

Pelsser, L.M., & Buitelaar, J. (2002), Gunstige invloed van een standaardeliminatiedieet op het gedrag van jonge kinderen met ADHD, een verkennend onderzoek [Favourable effect of a standard elimination diet on the behavior of young children with attention deficit hyperactivity disorder (ADHD): a pilot study], *Nederlands Tijdschrift voor Geneeskunde*, *146*, 2543-2547.

Penrose, R., & Hameroff, S. (1996), Conscious Events as Orchestrated Space-Time Selections, *Journal of Consciousness Studies*, *3 (1)*, 36-53.

Pfeuffer, J., Van de Moortele, P.-F. ,Yacoub, E., Shmuel, A., Adriany, G., Andersen, P., Merkle, H.,Garwood, M., Ugurbil, K., Hu, X., (2002), Zoomed Functional Imaging in the Human Brain at 7 Tesla with Simultaneous High Spatial and High Temporal Resolution, *Neuroimage 17 (1),* 272-86.

Poindexter, J. (2002), Total Information Awareness, *DARPA Tech 2002 Symposium*, http://www.darpa.mil/DARPATech2002/presentations/iao_pdf/slides/PoindexterIAO.pdf.

Polikar, R., Upda, L., Upda, S., &Honavar, V. (2001), Learn++: an incremental learning algorithm for supervised neural networks', *IEEE Trans. on Systems, Man and Cybernetics, Part C: Applications and Reviews*, *31 (4)*, 497-508.

Projectgroep Visie op de politiefunctie (2005), *Politie in ontwikkeling. Visie op de politiefunctie*, Den Haag: Raad van Hoofdcommissarissen, NPI, mei 2005 http://www.politie.nl/Overige/Images/33_143611.pdf.

Pylyshyn, Z.W. (1984), *Computation and Cognition: Towards a Foundation for Cognitive Science,* MIT Press.

Rasolzadeh, B., Björkman, M., & Eklundh, J.-O. (2006), An Attentional System Combining Top-Down and Bottom-Up Influences, *International Cognitive Vision Workshop (ICVW06), Graz, Austria*.

Remmelink, J. (1995), *Mr. D. Hazewinkel-Suringa's Inleiding tot de studie van het Nederlandse Strafrecht*, Arnhem: Gouda Quint

Renn, O., & Roco, M.C. (2006), Nanotechnology and the need for risk governance, *Journal of Nanoparticle Research 8 (2)*, 153-191. http://www.springerlink.com/content/y80541n7740785gm/fulltext.pdf

Rip, A. (2006), A Co-evolutionary Approach to Reflexive Governance – and its Ironies' in: Voss, J.P., Bauknecht, D., & Kemp, R. (eds.) *Reflexive Governance for Sustainable Development.*

Rip, A., & Te Kulve, H. (2007), Sociotechnical scenarios to support reflexive co-evolution: the approach of Constructive TA, *Yearbook of Nanotechnology in Society*, Dordrecht: Springer.

Robinson, M.B. (2003), *Why Crime? An Integrated Systems Theory of Antisocial Behaviour*

Roco, M.C., & Bainbridge, W.S. (eds.) (2002), *Converging Technologies for Improving Human Performance*, NSF/DOC – sponsored report, June 2002, http://wtec.org/ConvergingTechnologies/1/NBIC_report.pdf.

Roco, M.C. (2007a), National Nanotechnology Initiative - Past, Present, Future, In: Goddard, W.A., Brenner, D. , Lyshevski, S.E., & Lafrate, G., (eds.), *Handbook on Nanoscience, Engineering and Technology*, 2nd ed., London: Taylor and Francis, (3.1-3.26)

Roco, M.C. (2007b), New Frontiers for Nanotechnology, Presentation at *STW Conference Nieuwe Perspectieven*, Rotterdam, The Netherlands, October 4, http://www.stw-inschrijving.nl/DownloadPagina.aspx?page=downloaden

Rogers, E.M. (1995), *Diffusion of innovations*, New York: The Free Press

Schmidt, K.F., (2006) *Nanofrontiers*: *Visions for the Future of Nanotechnology*, Woodrow Wilson International Center for Scholars.

Selznick, P (1992) *The Moral Commonwhealth. Social Theory and the Promise of Community* Berkeley: University of California Press

Shoemaker, D.D., Lashkari, D.A., Morris, D., Mittmann, M., & Davis, R. (1996), Quantitative phenotypic analysis of yeast deletion mutants using a highly parallel molecular bar–coding strategy, *Nature Genetics 14*, 450 - 456.

Silberglitt, R., Antón, P.S. , Howell, D., & Wong, A., (2006), *The Global Technology Revolution 2020, In-Depth Analyses: Bio/Nano/Materials/Information Trends, Drivers, Barriers, and Social Implications*, Santa Monica, Ca: RAND National Defense Research Division , http://www.rand.org/.

Silva, A.J., Wang, Y., Paylor, R., Wehner, J., Stevens, C., & Tonegawa, S. (1992), Alpha calcium/calmodulin kinase II mutant mice: deficient long-term potentiation and impaired spatial learning', *Cold Spring Harb Symp Quant Biol*, *57*, 527-39.

Shors T.J., Miesegeas, G., Beylin, A., Zhao, M.,Riedel, T., & Gould, E. (2001), Neurogenesis in the adult is involved in the formation of trace memories, *Nature*, *410*, 372-376.

Smalley, R. (2001), Of Chemistry, Love, and Nanobots, *Scientific American*, *285,* 76-77.

Smalley, R. (2003a), Smalley Responds, *Chemical & Engineering News*, *81*, 39-40.

Smalley, R. (2003b), Smalley Concludes, *Chemical & Engineering News*, *81,* 41-42.

Smart, J.J.C. (2007), The Identity Theory of Mind, Edward N. Zalta (ed.), *The Stanford Encyclopedia of Philosophy (Summer 2007 Edition)*, http://plato.stanford.edu/archives/sum2007/entries/mind-identity/.

Smidt, H.J. (1881), *Geschiedenis van het Wetboek van Strafrecht. Volledige verzameling van regeeringsontwerpen, gewisselde stukken, gevoerde beraadslagingen, enz. Eerste deel*, Haarlem: H.D. Tjeenk Willink

Solove, D.J. (2004), *The Digital Person*, New York: New York University Press.

Spears, R., & M. Lea, M., (1004), Panacea or Panopticon? The hidden power in computer-mediated communication, *Communication Research, 21 (4)*, 427-459.

Stroes, E.S.G. (2007), Efficacy and Safety of Intramuscular Administration of AMT-010 (AAV-LPLS447X) in Lipoprotein Lipase Deficient Subjects, *10th Annual Meeting of the American Society of Gene Therapy*, Seattle, Washington, May 30 - June 3.

Sun, S., Murray, C.B., Weller, D., Folks, L., & Moser, A., (2000), Monodisperse FePt Nanoparticles and Ferromagnetic FePt Nanocrystal Superlattices, *Science*, *287*,

Swierstra, T. & Rip, A. (2007), Nano-ethics as NEST-ethics: patterns of moral argumentation about new and emerging science and technology, *NanoEthics 1*, 3-20

Tripp, S.L., Dunin-Borkowski, R.E., & Wei, A., (2003), Flux Closure in Self-Assembled Cobalt Nanoparticle Rings, *Angew. Chem. Int. Ed*, doi.wiley.com.

Van Est, R., Enzing, C., Van Lieshout, M., & Versleijen, A. (2006), *Welcome to the 21st century: Heaven, hell or down to earth?*, Annex 1 of Report IP/A/STOA/ST/2006-6 (ETAG, 2006).

Van Hamel, G.A. (1880), *De grenzen der heerschappij van het strafrecht*, oratie Amsterdam (UvA), Amsterdam: P.N. van Kampen & Zoon.

Van Wijck, P., De Wit, R., Kroon, R. & Van der Lee, R. (2007), *Justitie over morgen: Scenario's en strategieën voor 2015*, Den Haag: Ministerie van Justitie

Vedder, A.H. (1998), Het einde van de individualiteit? Datamining, groepsprofilering en de vermeerdering van brute pech en dom geluk, *Privacy & Informatie 3*, 115-120.

Vedder, A.H. (2001), The accountability of Internet access and service providers: Strict liability entering ethics? *Ethics and Information Technology 3 (1),* 67-74.

Vedder, A.H. (2004), KDD, Privacy, Individuality, and Fairness. In: R. Spinello, & H. Tavani (eds.), *Readings in CyberEthics*. Sudbury, Mass./Boston/Toronto/London/Singapore: Jones and Bartlett Publishers, 2004, pp. 462-470.

Vedder, A.H., & P. Blok (2005), Privacy en ICT. In: M. Lips, V. Bekkers & A. Zuurmond (ed.), *ICT en Openbaar Bestuur: Implicaties en uitdagingen van technologische toepassingen voor de overheid*, Utrecht: Lemma, 2005. (623-650)

Vedder, A.H., Van der Wees, L., Koops, B.J., & De Hert, P.(2007a), *Van privacyparadijs tot controlestaat? Misdaad- en terreurbestrijding in Nederland aan het begin van de 21ste eeuw*, Den Haag: Rathenau Instituut.

Vedder, A.H. (ed.) (2007b), *NGO Involvement in International Governance and Policy: Sources of Legitimacy*. Leiden: Martinus Nijhoff Publishers.

Vivehlin, K. (2003), Arguments for Incompatibilism. http://plato.stanford.edu/entries/incompatibilism-arguments/

Whitman, J. (2006), Governance challenges of technologiccal systems convergence, *Bulletin of Science, Technology & Society, 26 (5),* 398-409.

Willadsen, S.M. (1986), Nuclear transplantation in sheep embryos, *Nature, 320*, 63-65.

Wolf, S. (1993), *Freedom within Reason*, New York: Oxford University Press

Wood, D.M. (ed.), *A Report on the Surveillance Society For the Information Commissioner by the Surveillance Studies Network*, September 2006. http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf

Zippelius, R (2003), *Einführung in das Recht*, 4th ed., Heidelberg: C.F. Müller.

Appendix A: Project Organisation

A.1 Advisory committee ('begeleidingscommissie')

Prof. dr. H. Maassen van den Brink (chairman)	Universiteit van Amsterdam
Isa Brunetti	Justitie/directie Wetgeving
Siegfried Eschen	Justitie/directie Algemene Justitiële Strategie
Rob Hartman	ASML
Benjamin Jansen	Justitie/ Stafdirectie Coördinatie Vreemdelingenketen
Heleen Janssen	BZK/directie Constitutionele Zaken en Wetgeving
Erik Lanting	Justitie / directie Rechtshandhaving en Crim. Bestrijding, Afd. Criminaliteit en Veiligheid
Paul van der Lecq	Siemens
Wim Pelt	Defensie
Jan Piek	Justitie/Dienst Justitiële Inrichtingen (DCL)
Christianne de Poot	Justitie/Wetenschappelijk Onderzoek en Documentatie Centrum
Klaas Sanders	Justitie/directie Wetgeving
Marcel van der Steen	Justitie/Nederlands Forensisch Instituut
Albert Verweij	Justitie/Centraal Orgaan opvang Asielzoekers
Adri Voermans	BZK/directie Strategie
Willem Voogt	Justitie/Nationaal Coördinator Terrorisme-bestrijding
Paul van der Waals	Justitie JI/Concernstaf Bedrijfsvoering/Afd. Informatiemanagement
Clemens Willemsen	Justitie/directie Instrumentatie Rechts-pleging en Rechtshandhaving (Progis)
Linda van Wel	Justitie /directie Algemene Justitiële Strategie
Stavros Zouridis	Justitie /directie Algemene Justitiële Strategie

A.2 Interviewees (application group)

Siegfried Eschen	Justitie/directie Algemene Justitiële Strategie
Cees Kwanten	Politieacademie
Jan Piek	Justitie/Dienst Justitiële Inrichtingen (DCL)
Marcel van der Steen	Justitie/Nederlands Forensisch Instituut
Albert Verweij	Justitie/Centraal Orgaan opvang Asielzoekers
Adri Voermans	BZK/directie Strategie

Willem Voogt	Justitie/Nationaal Coördinator Terrorisme-bestrijding

A.3 Interviewees (scientific experts)

Prof. dr. ir. Albert van den Berg	Universiteit Twente/MESA+ institute for nanotechnology
Prof. dr. Wiel Hoekstra	Koninklijke Nederlandse Akademie van Wetenschappen
Prof.dr. Victor A.F. Lamme	Universiteit van Amsterdam, Cognitive Neuroscience Group
Prof.dr. John R. Long	Technische Universiteit Delft/Micro-elektronica & computer engineering

A.4 Websurvey participants

Dr.ir. Martin Bennink	Universiteit Twente, Enschede
Dr. Johan de Heer	Thales, Hengelo
Prof.dr. Peter de Knijff	Leiden Universitair Medisch Centrum
Prof.dr. Wiel Hoekstra	Koninklijke Nederlandse Akademie van Wetenschappen
Dr. André Hoogstrate	Nederlands Forensisch Instituut
Prof.dr. Catholijn Jonker	Technische Universiteit Delft
Dr.ir. Pieter Jonker	Technische Universiteit Delft
Dr. Ate Kloosterm	Nederlands Forensisch Instituut
Prof.dr.ir. Inald Lagendijk	Technische Universiteit Delft
Prof.dr. Victor Lamme	Universiteit van Amsterdam
Prof.dr. Lambert Schomake	Universiteit Groningen
Prof.dr. Arno Siebes	Centrum voor Wiskunde en Informatica, Amsterdam
Dr.mr. Ruben Sietsma	Korps Landelijke Politie Diensten / Universiteit Leiden
Prof.dr. Vinod Subramani	Universiteit Twente, Enschede
Prof.dr. Jan Treur	Vrije Universiteit, Amsterdam
Prof.dr. Frank van Harm	Vrije Universiteit, Amsterdam

A.5 Participants technology workshop to discuss websurvey results

Maarten Blom	Nederlands Forensisch Instituut
Martijn van Boxtel	Politie Rotterdam Rijnmond
Anick van de Craats	Nederlands Forensisch Instituut
Prof.dr. Edward de Haan	neuropsychology – Universiteit Utrecht
Dr. Johan de Heer	director T Exchange – Thales

Prof.dr. Paul de Hert	Tilburg University
Ruud Hoefnagel	Politie Rotterdam Rijnmond
Dr. Ir. Hans Kanger	virus sensors – BMTI
Prof. Dr. Manfred Kayser	forensic molecular biology – Erasmus UMC
Prof. Dr. Peter de Knijff	population and evolutionary genetics – Leiden UMC
Dr.Mr. Ruben Sietsma	University of Leiden / KLPD
Prof.Dr. Sabeth Verpoorte	pharmaceutical analysis – Rijksuniversiteit Groningen
Dr.ir. Edward Faber	Telematica Instituut (project team)
Dr. Henk de Poot	Telematica Instituut (project team)
Dr.ir. Wouter Teeuw	Telematica Instituut (project team)
Dr. Anton Vedder	Tilburg University (project team)

A.6 Participants workshop on impact analysis

Martijn van Boxtel	Politie Rotterdam Rijnmond
Philip Breij	Universiteit Twente, Enschede
Wibren van der Burg	Tilburg University
Anton Ekker	Solicitor SOLV
Rop Gonggrijp	Founder XS4ALL
Joris van Hoboken	University of Amsterdam / Institute for Information Law
Rob van den Hoven van Genderen	Vrije Universiteit, Amsterdam
Bart Jacobs	Radboud University, Nijmegen
Arno Lodder	Vrije Universiteit, Amsterdam
Bart Schermer	ECP.NL
Aernout Schmidt	University of Leiden
Dr.Mr. Ruben Sietsma	KLPD
Pieter Vermaas	Delft University of Technology
Bart Custers	Tilburg University, Capgemini (project team)
Bärbel Dorbeck-Jung	Universiteit Twente (project team)
Henk de Poot	Telematica Instituut (project team)
Arie Rip	Universiteit Twente (project team)
Wouter Teeuw	Telematica Instituut (project team)
Anton Vedder	Tilburg University (project team)

A.7 Acknowledgements

The project team owes many thanks to all those who have unselfishly put time and enthusiasm into this project. In particular we want to acknowledge the members of the advisory committee and the participants of interviews, web survey and workshops, as listed in the previous sections. Also we want to acknowledge Pierre Morin and Bernard Verlaan of the *Commissie van Overleg Sectorraden*[50] for providing us with all kinds of input information, and our colleagues Rogier Brussee and Patrick Strating from Telematica Instituut for reviewing (parts of) this report.

[50] http://www.toekomstverkennen.nl/

Appendix B: Results of the web survey

We performed a so-called 'web survey' (using tools from www.surveyworld.net) to evaluate our initial ideas on:

1 how realistic the expected developments in nanotechnology, biotechnology, ICT and cognition are, and

2 how the technology developments may converge into expected applications for our three case studies.

The survey has been opened on June 18th and closed on June 25th, 2007. The survey has been sent out to a selected group of 47 persons, among which 6 members of the project team (who did not respond to the survey). The remaining 41 persons are all professors or experts from a technology or application domain. From this group, 16 experts (39%) completely filled out the survey, a single person answered not to participate and the remaining 24 persons did not reply within the one-week period the survey was open for response. Among the 41 selected persons was also a group of 12 experts who joined a physical session (workshop) on June 27th in The Hague to discuss the survey results. From this subgroup of 12 experts, 3 experts (25%) are among the 16 respondents who filled out the survey.

In section B1 of this Appendix, the participants who filled out the survey express their familiarity on the topic; in section B2 we list the results on the questions addressing the NBIC technology domains; and in section B3 we list the results on the questions addressing the application domain.

B.1 Part I: Survey participants

Answer to question: To what extent do you regard yourself as an expert in the following technology fields (a) nanotechnology, (b) biotechnology, (c) information technology, (d) cognitive sciences

	novice	average	expert	n
Nanotechnology	11	0	3	14
Biotechnology	9	1	5	15
Information technology	3	3	9	15
Cognitive sciences	7	2	5	14

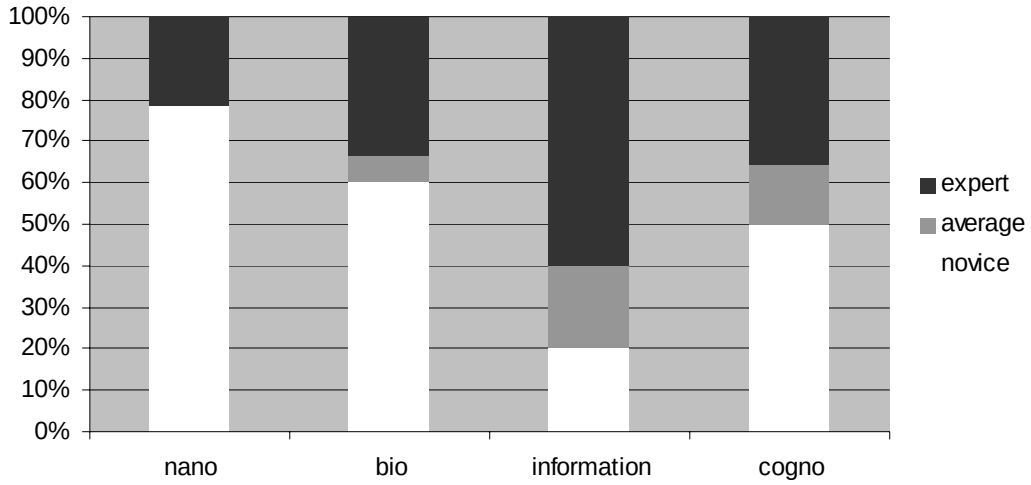


Figure 37: Expertise fields of the web survey participants.

Answer to question: To what extent are you familiar with the following cases?

- Monitoring and following objects and persons and remotely taking action in case of undesired movements
- Improving and developing forensic research
- Profiling, indentifying and observing persons with an assumed security risk

	unfamiliar	no opinion	familiar	n
Monitoring and immediate action	6	2	7	15
Forensic research	5	2	9	16
Profiling and identifying persons	4	4	7	15

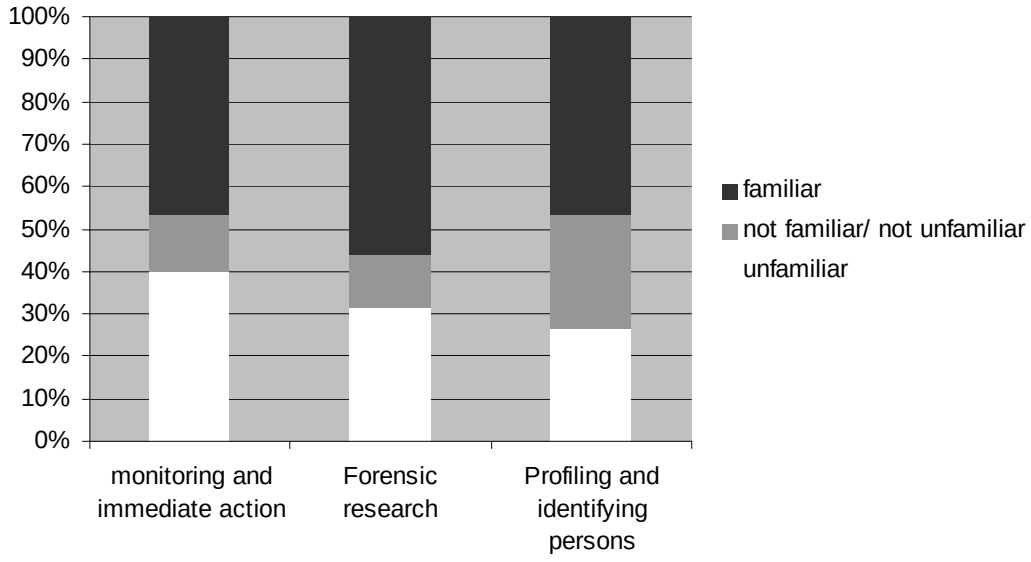


Figure 38: Familiarity with the cases of the web survey participants.

B.2 Part II: Technological developments

Answer to the question: In what time frame are the following nanotechnologies mature enough to be applied in the security domain? (<5 year <10 year <15 year >15 year)

- *Reactive ('smart') materials capable to change their properties in response to different external changes (like temperature)*
- *Micro-chip technology with sub 10 nm structures of active components*
- *Nano-manipulators for nano molecular assembly*
- *Nano imaging tools for visualisation of nanoscale structures*

NANO	< 5 year	<10 year	<15 year	>15 year	n
Smart materials	28.6%	57.1%	14.3%	0.0%	7
Micro chips	12.5%	37.5%	50.0%	0.0%	8
Nano manipulators	14.3%	28.6%	42.9%	14.3%	7
Nano imaging	50.0%	25.0%	25.0%	0.0%	8

NANO cumulative	< 5 year	<10 year	<15 year	>15 year	n
Smart materials	28.6%	85.7%	100.0%		7
Micro chips	12.5%	50.0%	100.0%		8
Nano manipulators	14.3%	42.9%	85.7%	100.0%	7
Nano imaging	50.0%	75.0%	100.0%		8

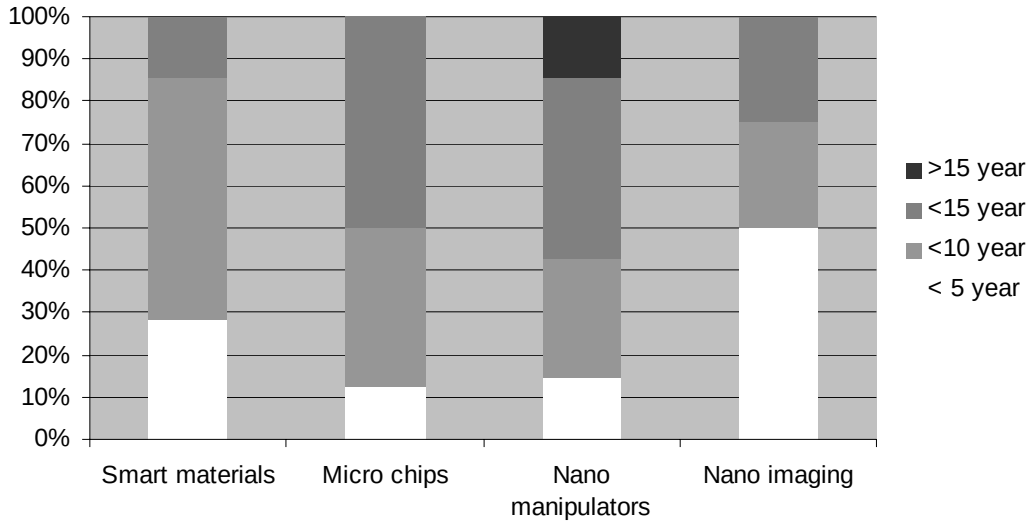


Figure 39: Expected applicability of nanotechnology in the security domain.

Answer to the question: Which (other) important Nanotechnologies are important for the coming 15 years in general and for the public security sector in particular?
The answers are:

- Nano-computing architectures
- Nanodiagnostics; nanoparticles for imaging and diagnostics at the single molecule level
- Nano-particles for biosensing, or drug delivery
- Not for public security but for implementing biocompatible neural implants with cognitive capabilities, nanotechnology will be an essential ingredient. Micron-level electrode arrays will be too cumbersome, risky and will not provide the necessary communication bandwidth.
- Portable lab-on-a-chip devices passport containing the owners DNA profile Quick screening methods to verify the identity of persons

Answer to the question: How long before the following biotechnologies are mature enough to be applied in the security domain? (<5 year <10 year <15 year >15 year)

- *Accurate, fast and easy to use DNA analysis tools*
- *Gene passports presenting a person's individual genome*
- *Genetic profiling, which lead to understanding the evolution of some diseases, and to better treatments*

BIO	< 5 year	<10 year	<15 year	>15 year	n
DNA analysis tools	63.6%	36.4%	0.0%	0.0%	11
Gene passports	0.0%	45.5%	45.5%	9.1%	11
Genetic profiling	25.0%	33.3%	25.0%	16.7%	12

BIO cumulative	< 5 year	<10 year	<15 year	>15 year	n
DNA analysis tools	63.6%	100.0%			11
Gene passports	0.0%	45.5%	90.9%	100.0%	11
Genetic profiling	25.0%	58.3%	83.3%	100.0%	12

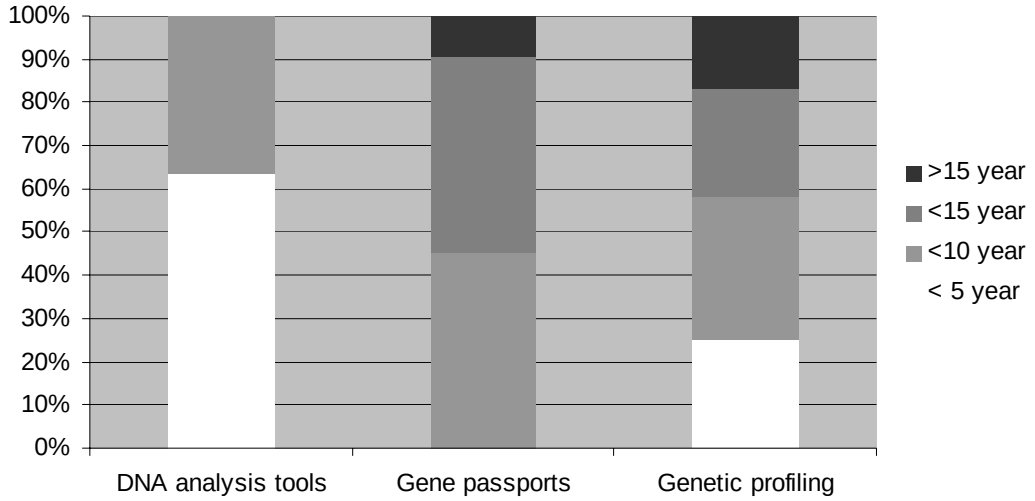


Figure 40: Expected applicability of biotechnology in the security domain.

Answer to the question: Which (other) important Biotechnologies are important for the coming 15 years in general and for the public security sector in particular?
The answers are:

- Fast detection methods for pathogens that could be used as biological weapons
- Genetic therapy Genetic therapy in utero Non human DNA typing technologies
- Model-based molecular design tools which combine high-performance computing and array/assay techniques in a closed experimentation loop.
- Single molecule protein detection /identification methods
- Understanding computing / life within the cell

Answer to the question: How long before the following information technologies are mature enough to be applied in the security domain? (<5 year <10 year <15 year >15 year)

- *Quantum computing*
- *Miniaturisation will reach a near- to- atomic levels with processors with 5 nm gates becoming commercially viable*
- *Electronic appliances of various kinds will be printable on functional polymers with desktop-printers.*
- *Long lasting batteries based on fuel cells*
- *Power-scavenging technologies integrated so that these sensor networks ('smart dust') and implantable devices stay functioning without battery replacement*
- *Body sensors to monitor blood flow and hormone level, and related to this, implantable drug dispensers*
- *Household robotics*
- *New computing paradigms such as chemical, biological or physical Turing machines*
- *Sensor networks spread around in the living body, in vitro in living cells, in the air*

INFO	< 5 year	<10 year	<15 year	>15 year	n
Quantum computing	0.0%	15.4%	15.4%	69.2%	13
Miniaturisation	0.0%	0.0%	90.0%	10.0%	10
Printable appliances	11.1%	33.3%	33.3%	22.2%	9
Fuel cells	10.0%	50.0%	10.0%	30.0%	10
Power scavenging	0.0%	30.0%	60.0%	10.0%	10
Body sensors	28.6%	35.7%	35.7%	0.0%	14
Household robots	21.4%	14.3%	35.7%	28.6%	14
New computing paradigms	0.0%	20.0%	10.0%	70.0%	10
Sensor networks	0.0%	16.7%	50.0%	33.3%	12

INFO cumulative	< 5 year	<10 year	<15 year	>15 year	n
Quantum computing	0.0%	15.4%	30.8%	100.0%	13
Miniaturisation	0.0%	0.0%	90.0%	100.0%	10
Printable appliances	11.1%	44.4%	77.8%	100.0%	9
Fuel cells	10.0%	60.0%	70.0%	100.0%	10
Power scavenging	0.0%	30.0%	90.0%	100.0%	10
Body sensors	28.6%	64.3%	100.0%		14
Household robots	21.4%	35.7%	71.4%	100.0%	14
New computing paradigms	0.0%	20.0%	30.0%	100.0%	10
Sensor networks	0.0%	16.7%	66.7%	100.0%	12

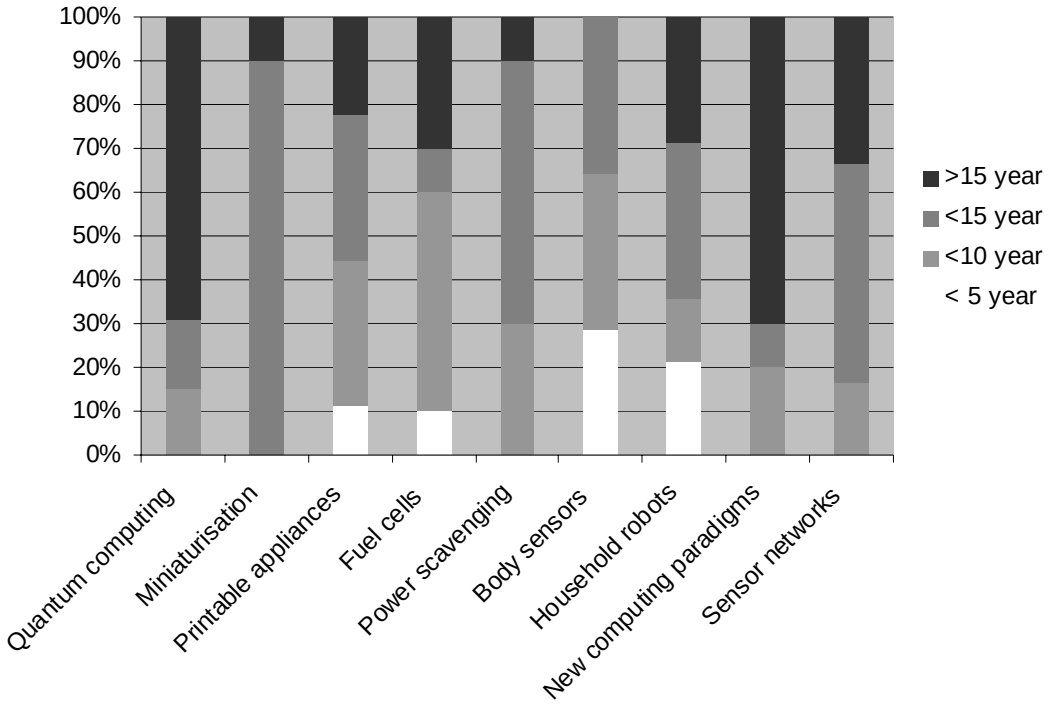


Figure 41: Expected applicability of information technology in the security domain.

Answer to the question: Which (other) important Information technologies are important for the coming 15 years in general and for the public security sector in particular?
The answers are:

- Data integration technology to enable combination of multiple data sources
- Adaptive and natural human computer interfaces

- By far the most important is still Moore's law, i.e., fast increasing: - bandwidth - storage capacity - processing power
- Data mining and financial transaction tracking.
- Micro /nano in vitro robots

Answer to the question: How long before the following cognition technologies are mature enough to be applied in the security domain? (<5 year <10 year <15 year >15 year)

- *Computational models of human perception*
- *Reading intentions from facial expressions and micro movements*
- *Contextual models of aggression*
- *Early warning systems for behavioural derailing*
- *Understanding the relation between neural processes (either "normal", or "altered" through drugs or illness), and the conscious experience*

COGNO	< 5 year	<10 year	<15 year	>15 year	n
Models human perception	15.4%	7.7%	53.8%	23.1%	13
Reading intentions	23.1%	30.8%	23.1%	23.1%	13
Models of aggression	23.1%	38.5%	30.8%	7.7%	13
Early Warning Systems	16.7%	41.7%	8.3%	33.3%	12
Understand relation neural processes and experience	0.0%	27.3%	27.3%	45.5%	11

COGNO cumulative	< 5 year	<10 year	<15 year	>15 year	n
Models human perception	15.4%	23.1%	76.9%	100.0%	13
Reading intentions	23.1%	53.8%	76.9%	100.0%	13
Models of aggression	23.1%	61.5%	92.3%	100.0%	13
Early Warning Systems	16.7%	58.3%	66.7%	100.0%	12
Understand relation neural processes and experience	0.0%	27.3%	54.5%	100.0%	11

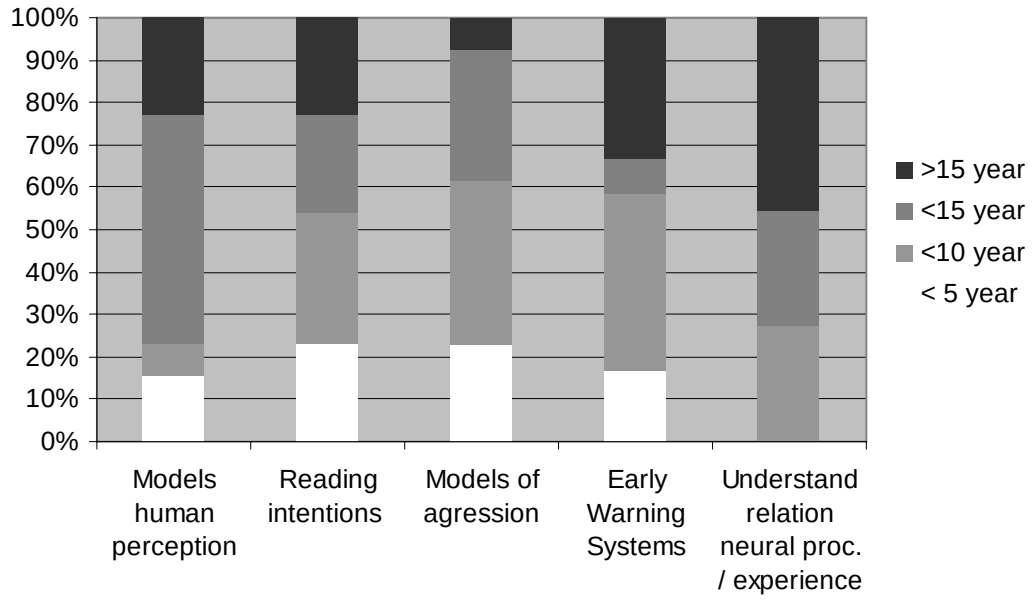


Figure 42: Expected applicability of cognition sciences in the security domain.

Answer to the question: Which (other) important developments in Cognitive science are important for the coming 15 years in general and for the public security sector in particular?

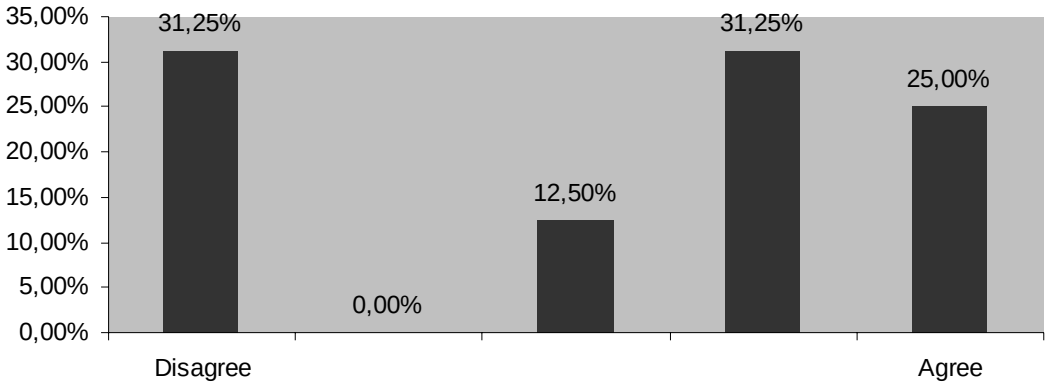
The answers are:

- Behavioural guidance systems (gps+context sensitive risk warnings), human-error reduction technologies, multimodal information integration.
- Brain computer interfaces
- 'Brain reading' (judging one's thoughts, perceptions or memories from brain imaging methods such as fMRI, EEG/MEG) Brain signal related lie-detection
- None, I do not see this field as being reliable and thus important
- Understanding learning on various abstraction layers detailed understanding of the 'hardware architecture' of the brain

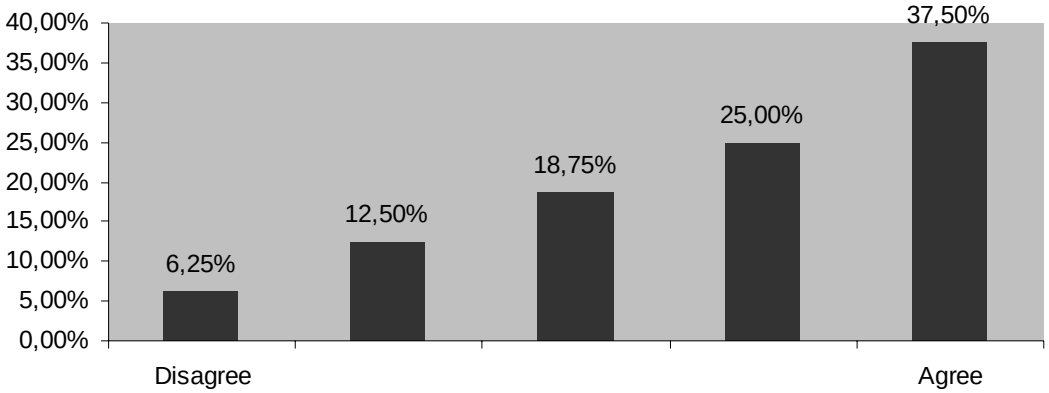
B.3 Part III: Application cases

B.3.1 Case 1: monitoring and intermediate action

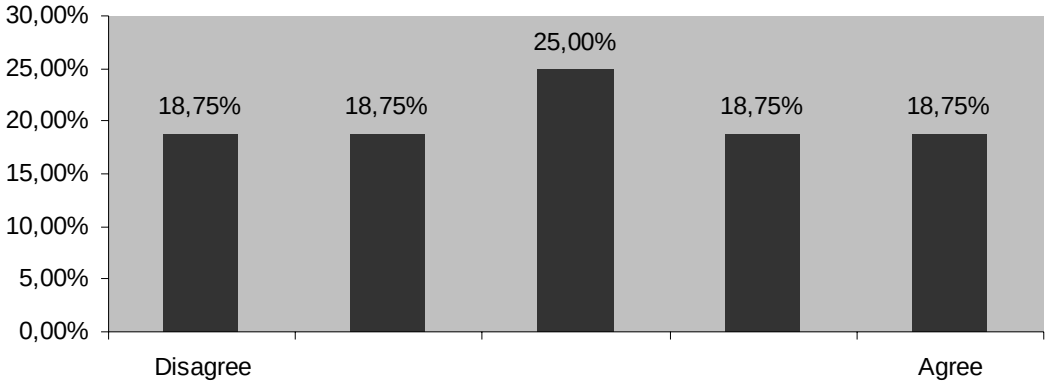
Answer to the question: What is your opinion on the following statements?



- *Persons have more and more identities, both in real life and in the virtual world (average 3.2 on a scale of 1=disagree to 5=agree)*



- *People will trade privacy for increased (perceived) social security (average 3.8)*



- *People will share their location information with the authorities (average 3.0)*

Comments:

– For the last point: I'm not sure that this is what people want, but it is what they do already. Mobile phone data gives a pretty good clue now and this will become better.
– Nanobiotechnology for the implanting device
– The ethical and social consequences of such monitoring need to be discussed in detail
– The last question: it depends on what their perceived reliability and trustworthiness of these authorities is.
– Too general, there are no "people"

– You cannot say that. This is situation dependent! Sometimes you want it sometimes not.

Which technological breakthroughs on your field of expertise will have a profound impact on the case monitoring and intermediate action?
The answers are:
– Artificial perception, making it possible to detect the environment a person is in.
– As a data miner, I should point to ever better ways to predict what is going to happen next. For example, distinguishing whether someone "disappeared" voluntarily from when this was done by force.
– Cooperative heterogeneous networks of humans and artificial actors, e.g., networks for the policy, ambulance, customs, etc.
– Intelligent data integration between different databases
– Interaction of nanosystems with cells (neurons)
– Networked tracking camera's that do not output images, but only observations and warnings in depersonalised matter, such as wireframes of persons or observations in words.
– Real time geographic monitoring

Answer to the question: How long will it take before the following innovations become reality?
– *Tagging prisoners detained during her Majesty's pleasure ('TBS') with implanted RFID tags*
– *Positioning technology combined with bio- and nano sensors enable tracking and tracing individuals.*
– *Movement of cars or persons ('knee-lock') can be blocked either manually from a distance or automatically based on sensor information (like entering a virtual no trespassing border).*
– *Electronically controlled animals can be sent out for surveillance (or for attack).*
– *Converging technologies make it possible to forecast who will become recidivist and who will not.*
– *Converging technologies make it possible to influence the perceived recollection of persons (to be used therapeutically).*
– *Influencing behaviour by brain implants.*
– *Prison without walls, i.e., a virtual imprisonment enforced by technology.*
– *Selective chemical or biological substances only affect people with certain genetic traits.*

Case 1: monitoring and immediate action	< 5 year	<10 year	<15 year	>15 year	n
Tagging prisoners	42.9%	35.7%	21.4%	0.0%	14
Tracking & tracing	16.7%	33.3%	8.3%	41.7%	12
Remote locking	28.6%	35.7%	28.6%	7.1%	14
Electronically controlled animals	0.0%	18.2%	27.3%	54.5%	11
Forecasting of recidivists	10.0%	10.0%	20.0%	60.0%	10
Influence the perceived recollection	12.5%	12.5%	0.0%	75.0%	8
Influence behaviour by brain implants	0.0%	18.2%	0.0%	81.8%	11
Prison without walls	7.7%	30.8%	15.4%	46.2%	13
Selective chemical or biological substances	0.0%	20.0%	30.0%	50.0%	10

Case 1 cumulative	< 5 year	<10 year	<15 year	>15 year	n
Tagging prisoners	42.9%	78.6%	100.0%		14
Tracking & tracing	16.7%	50.0%	58.3%	100.0%	12
Remote locking	28.6%	64.3%	92.9%	100.0%	14
Electronically controlled animals	0.0%	18.2%	45.5%	100.0%	11
Forecasting of recidivists	10.0%	20.0%	40.0%	100.0%	10
Influence the perceived recollection	12.5%	25.0%	25.0%	100.0%	8
Influence behaviour by brain implants	0.0%	18.2%	18.2%	100.0%	11
Prison without walls	7.7%	38.5%	53.8%	100.0%	13
Selective chemical or biological substances	0.0%	20.0%	50.0%	100.0%	10

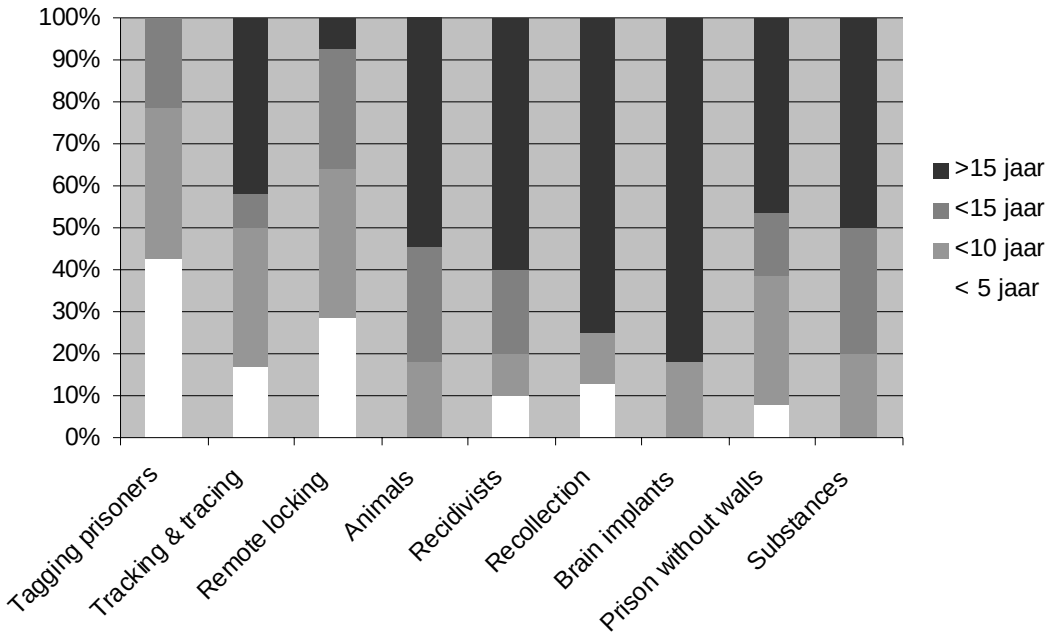
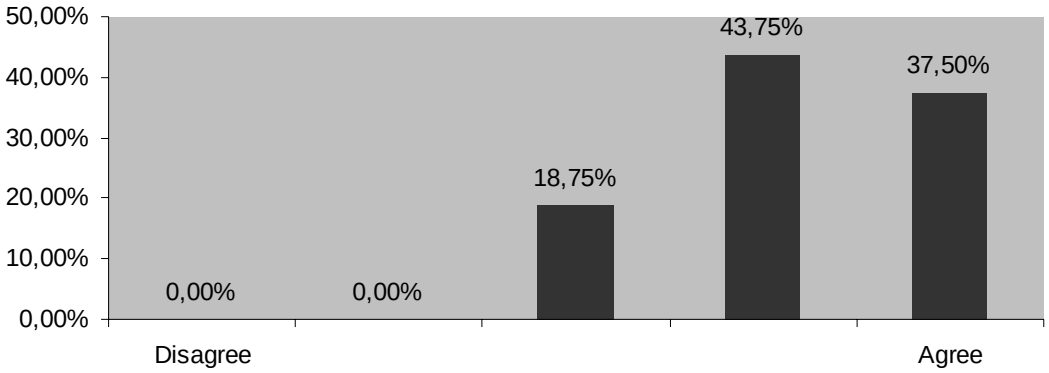


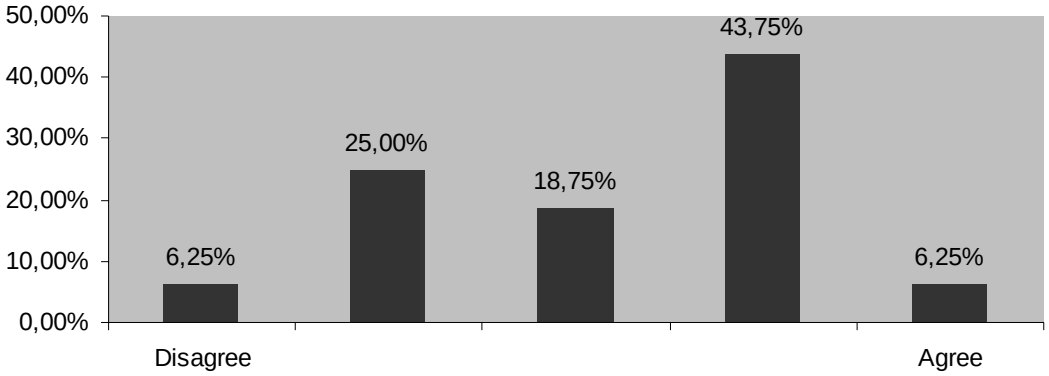
Figure 43: Expected applicability of technology for monitoring and immediate action.

B.3.2 Case 2: forensic research

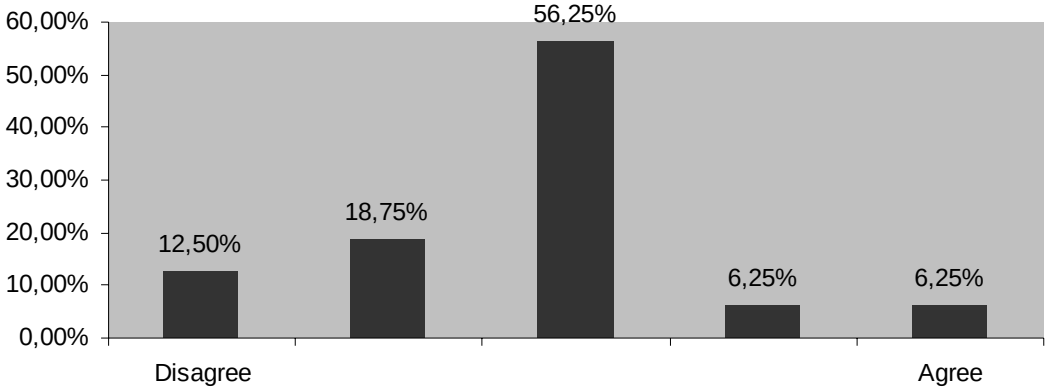
Answer to the question: What is your opinion on the following statements?



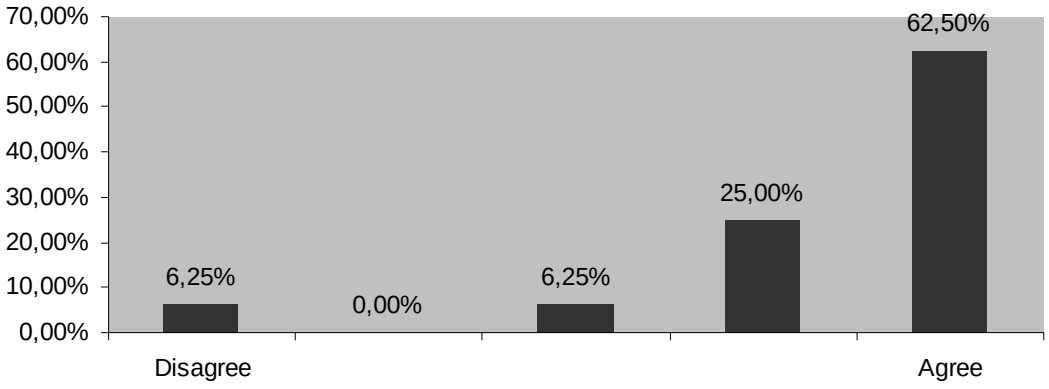
- *Traces are becoming smaller and smaller - a single cell may be enough for analysis (average 4.2)*



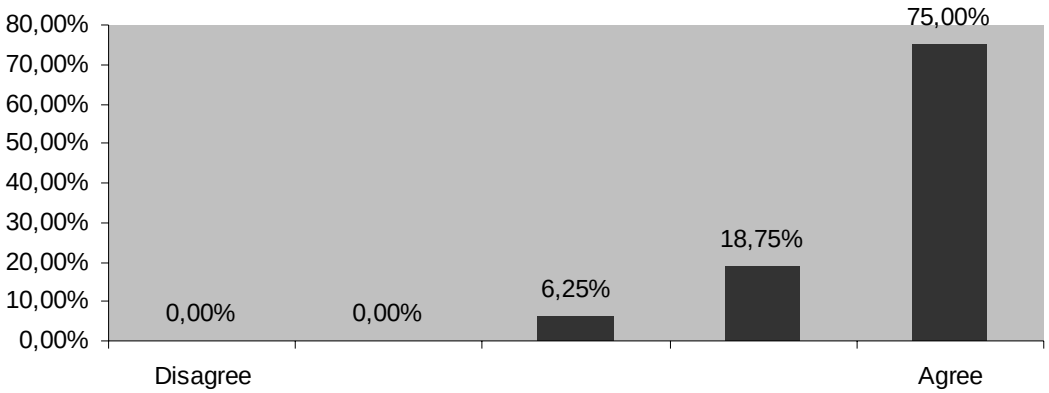
- *Technology which used to be available in specialised labs (like the NFI) will become available to everyone - with tools becoming smaller in size (average 3.2)*



- *Materials become more perfect and herewith less distinguishable (average 2.8)*



- *DNA databases will be internationally coupled (average 4.4)*



- *Criminality shifts towards the virtual world as well (average 4.7)*

Comments:
– I don't understand the third point, distinguishable from what?

Which technological breakthroughs on your field of expertise will have a profound impact on forensic research?
The answers are:
– Again, it will be the development of analysis methods that can produce accurate models based on the vast amounts of data that can and will be collected.
– Brain reading Brain signal guided lie-detection
– Fast and massive whole sequencing technologies enabling reliable DNA analyses of even the most complicated mixed DNA samples.
– further linking of DNA technology and information technology
– Introduction of SNP typing technologies Dry analysis of DNA
– Nanoparticles are dangerous when inhaled!!! like asbestos. Don't pollute the world with it.
– Nanoparticle imaging and diagnostics; optical sensing devices
– Non-suppressible neural reactions on the presentation of crime-scene related pictorial information: low-cost MRI devices.

– Pattern recognition techniques, e.g., identification of authors of handwritten material, patterns of behaviour.

Answer to the question: How long will it take before the following innovations become reality?

– *Biotechnology provides mechanisms of cellular recognition for forensic research.*
– *Nanotechnology-based sprayers can be used to sprinkle a room and find the tiniest traces.*
– *Nanotechnology enables the production or treatment of objects (like clothes, cars, et cetera) so that hardly any trace can still be found.*
– *Portable DNA profiling devices*

Case 2: forensic research	< 5 year	<10 year	<15 year	>15 year	n
Cellular recognition	20.0%	50.0%	20.0%	10.0%	10
Sprayers to find the tiniest traces	0.0%	28.6%	28.6%	42.9%	7
Treatment of objects	0.0%	28.6%	28.6%	42.9%	7
Portable DNA profiling devices	21.4%	21.4%	35.7%	21.4%	14

Case 2 cumulative	< 5 year	<10 year	<15 year	>15 year	n
Cellular recognition	20.0%	70.0%	90.0%	100.0%	10
Sprayers to find the tiniest traces	0.0%	28.6%	57.1%	100.0%	7
Treatment of objects	0.0%	28.6%	57.1%	100.0%	7
Portable DNA profiling devices	21.4%	42.9%	78.6%	100.0%	14

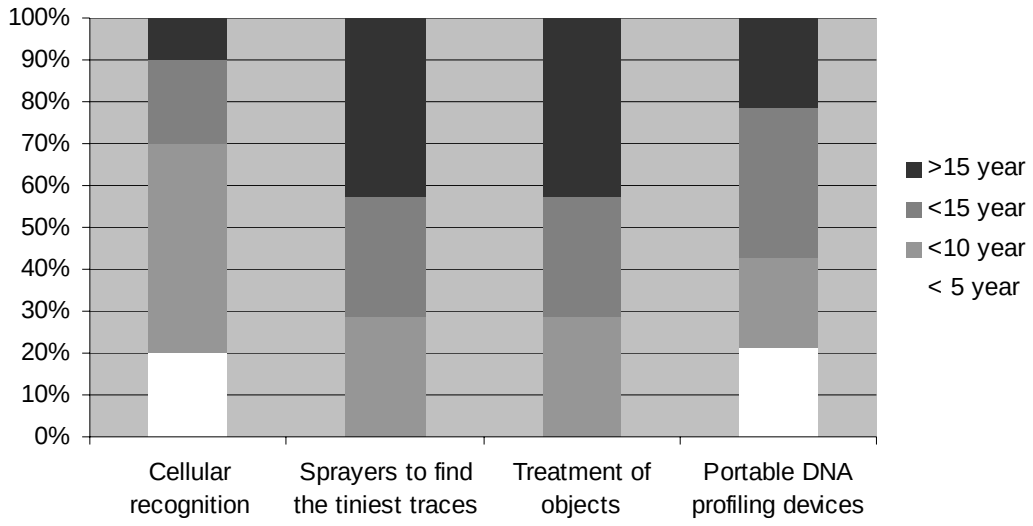
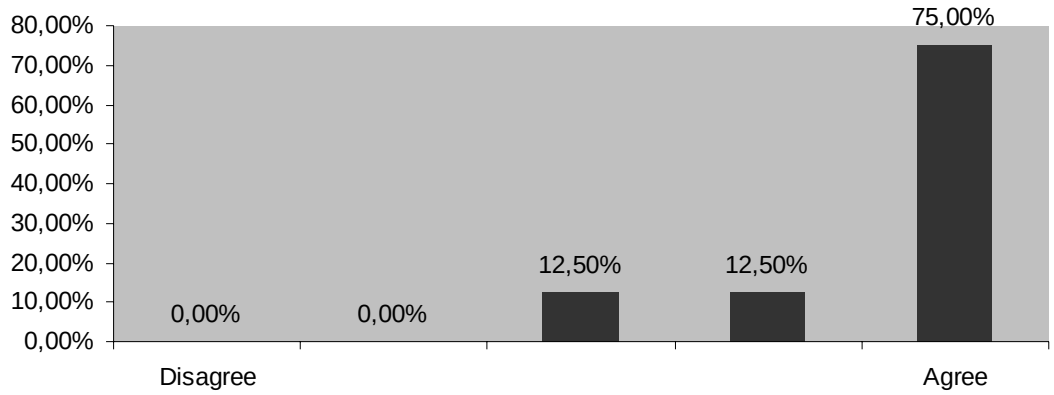


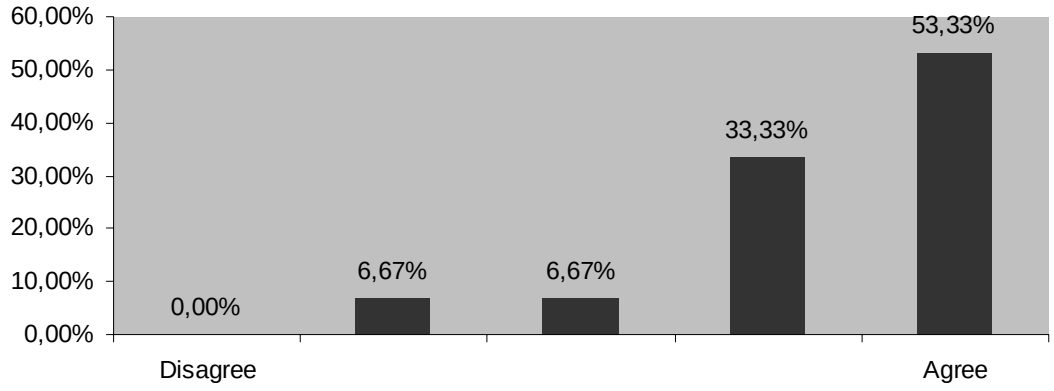
Figure 44: Expected applicability of technology for forensic research.

B.3.3 Case 3: profiling and identification

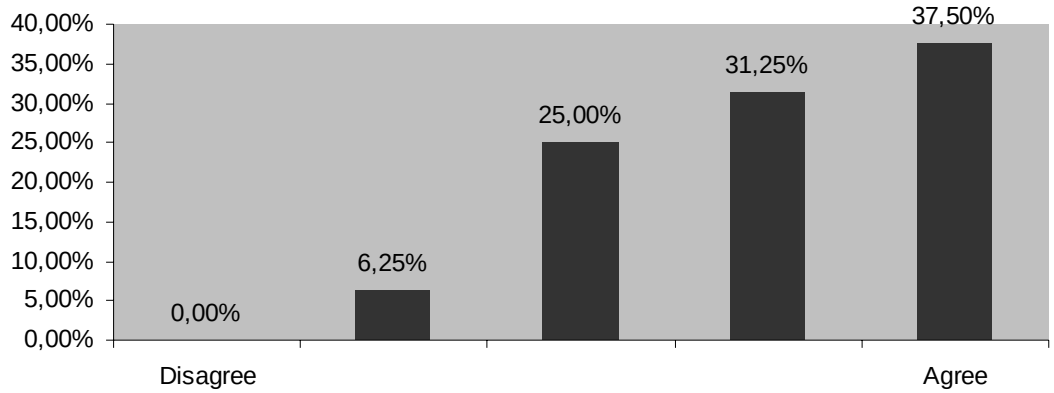
Answer to the question: What is your opinion on the following statements?



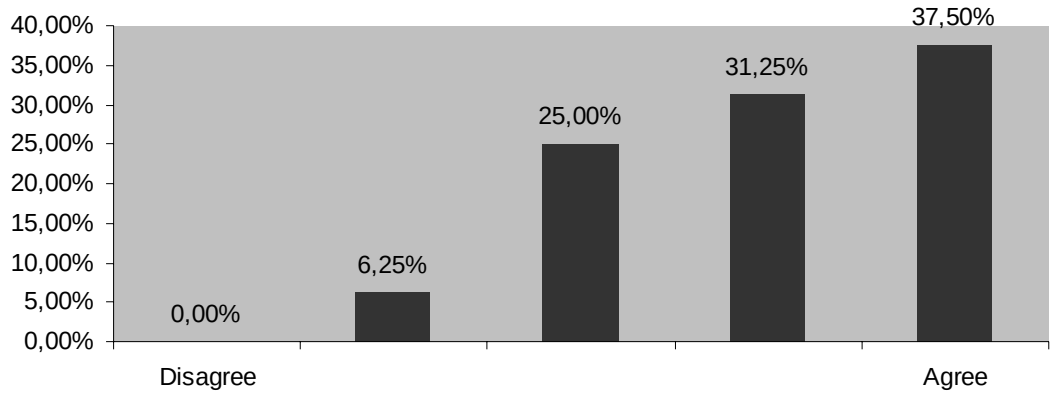
- *People leave more and more traces in the virtual world by browsing on Internet, using their mobile phone, wearing RFID tags with them, or being observed by cameras (average 4.6)*



- *The amount of data registered about persons and objects is growing enormously (average 4.3)*



- *Passports will contain DNA based information (average 4.0)*



- *Intelligent video surveillance (face recognition) will also be possible in difficult circumstances (average 4.0)*

Comments:
- Active vision and optomechanical camera devices will allow for high-quality panning and zooming in crowds, simultaneously tracking several individual persons (faces).
- Last question: (provisionally) as early warning system
- There is a better chance of recognizing people based on biological motion patterns in the case of difficult circumstances (bad lighting etc)

Which technological breakthroughs on your field of expertise will have a profound impact on risk analysis?
The answers are:
- Again, it will be the development of analysis methods that can produce accurate models based on the vast amounts of data that can and will be collected.
- Artificial face recognition Artificial body movement recognition Artificial aggression recognition
- DNA profiles combined with actual behavioural evidence can be used to generate risk profiles using Bayesian belief networks
- Fusion of information from various modalities, e.g., combining speech information with video images. Normal spectrum analysis of video footage, but also infrared etc.
- Machine perception and machine cognition; what is going on in the scene; logic understanding of the scene. Also for household / care robots
- None I can think off

Answer to the question: How long will it take before the following innovations in profiling and identification become reality?
- *Persons are continuously monitored both in the virtual and real world using ICT-, nano- or bio-enabled (wearable) sensors.*
- *A person's sensitivity to criminal behaviour can be derived from DNA.*

- *Due to enhanced man-machine (and brain-computer) interfaces, people leave so many traces that from the information stored on Internet, we know who they are and what they think.*
- *So-called '(remote) brain reading' can be used for profiling or identification purposes.*
- *Face recognition is reliable enough to be used to partly replace human intelligence*
- *Total information awareness: the ability to record and correlate all possible electronic traces left by a person, and the extraction of additional information, such as abnormal behavioural patterns*
- *Event prediction based on continuous observation of persons with an assumed security risk.*

Case 3: Profiling and identification	< 5 year	<10 year	<15 year	>15 year	n
Persons continuously monitored	9.1%	45.5%	27.3%	18.2%	11
Behaviour derived from DNA	10.0%	30.0%	0.0%	60.0%	10
Internet tells who we are	9.1%	9.1%	45.5%	36.4%	11
Brain reading	0.0%	9.1%	27.3%	63.6%	11
Face recognition	0.0%	36.4%	27.3%	36.4%	11
Total information awareness	16.7%	8.3%	66.7%	8.3%	12
Event prediction	18.2%	45.5%	36.4%	0.0%	11

Case 3 cumulative	< 5 year	<10 year	<15 year	>15 year	n
Persons continuously monitored	9.1%	54.5%	81.8%	100.0%	11
Behaviour derived from DNA	10.0%	40.0%	40.0%	100.0%	10
Internet tells who we are	9.1%	18.2%	63.6%	100.0%	11
Brain reading	0.0%	9.1%	36.4%	100.0%	11
Face recognition	0.0%	36.4%	63.6%	100.0%	11
Total information awareness	16.7%	25.0%	91.7%	100.0%	12
Event prediction	18.2%	63.6%	100.0%	100.0%	11

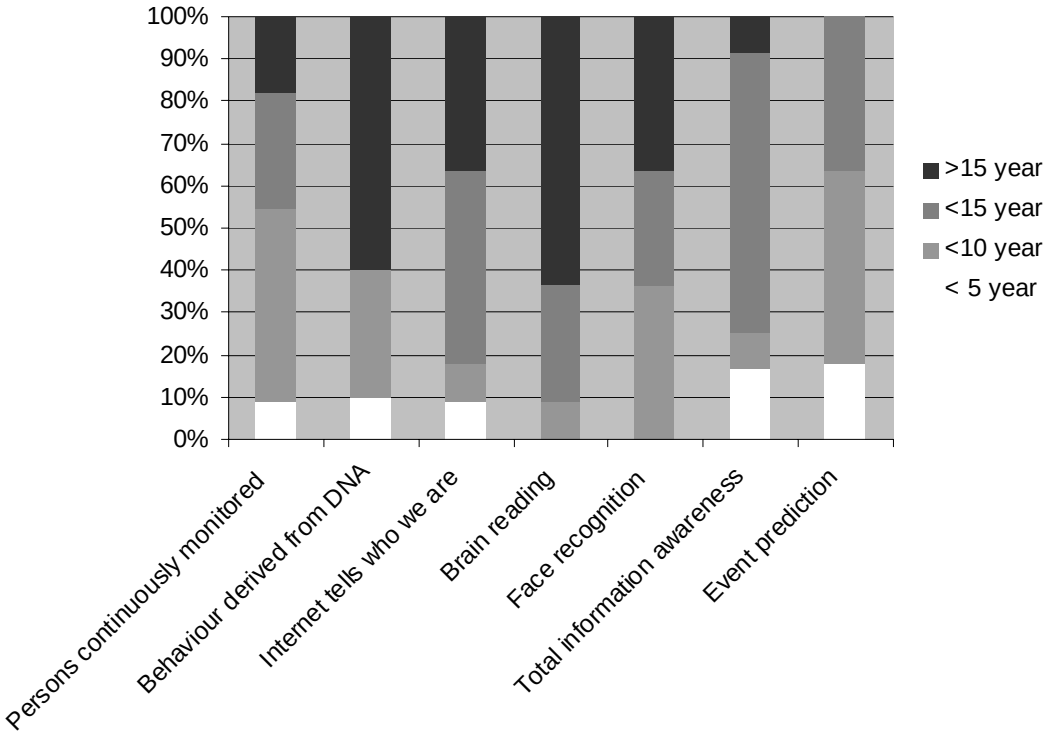


Figure 45: Expected applicability of technology for profiling and identification.

Comments:

- 'Dit zijn iha geen ja/nee vragen. Bijv. laatste vraag: hoeveel kans op succes wil je?'
- 'Een paar vragen die ver van mijn bed liggen.'
- Face recognition: it depends on the details of the actual application (pass photo vs. surveillance cam. context).
- How long will it take before incidents are reported of people that blocked out of some activities because of a mix up in the gathered information about them and other people?